INFORME DE AUDITORÍA

DEFINITIVO

Auditoría al Proceso de Gestión de Tecnología de la Información y las Comunicaciones

OFICINA DE CONTROL INTERNO

JULIE ANDREA SOTO LAVERDE
JEFE DE LA OFICINA DE CONTROL INTERNO

EQUIPO AUDITOR
RIGOBERTO ANDRES VACA PARDO

PERIODO EVALUADO
(VIGENCIA 2024 Y 2025)

FECHA DEL INFORME
(25 de mayo de 2025)

Contenido

1. INFORMACIÓN GENERAL 3
1.1. **DESTINATARIOS DE LA AUDITORÍA** 3
1.2. EQUIPO AUDITOR 3
2. OBJETIVO DE LA AUDITORÍA 3
3. ALCANCE DE LA AUDITORÍA 3
4. CRITERIOS 3
5. METODOLOGÍA 4
7. RESUMEN EJECUTIVO DE LOS RESULTADOS DE LA AUDITORIA 5
8. RESULTADOS DETALLADOS DE LA AUDITORIA 6
8.1. COMPONENTE AMBIENTE DE CONTROL 6
8.2 COMPONENTE EVALUACIÓN DEL RIESGO 14
8.3 COMPONENTE ACTIVIDADES DE CONTROL 24
8.4 COMPONENTE INFORMACIÓN Y COMUNICACIÓN 51
8.5 COMPONENTE ACTIVIDADES DE MONITOREO 55

1. INFORMACIÓN GENERAL

1.1. DESTINATARIOS DE LA AUDITORÍA

La presente auditoria tiene como destinatarios principales:

Secretario General
Coordinador de Grupo de Gestión de Tecnología
Oficina de Planeación y Gestión Internacional – Grupo de Gestión y Desempeño.
Subdirección Administrativa y Financiera - Grupo de Gestión Contractual.

1.2. EQUIPO AUDITOR

El equipo auditor asignado para llevar a cabo la presente evaluación es el siguiente:

Julie Andrea Soto Laverde - Jefe de Oficina de Control Interno
Rigoberto Andrés Vaca Pardo - Contratista.

2. OBJETIVO DE LA AUDITORÍA

Revisar y evaluar la eficacia la gestión de riesgo, control y gobierno del proceso Gestión de Tecnología de la Información y las Comunicaciones del Ministerio de Minas y Energía y los recursos del proyecto de inversión asociado al Fortalecimiento de las Capacidades tecnológicas.

3. ALCANCE DE LA AUDITORÍA

Realizar auditoría integral a la gestión del proceso de Gestión de Tecnología de la Información y las Comunicaciones, así como la evaluación de los controles, procedimientos e instructivos respectivos, correspondientes al período comprendido entre la vigencia 2024 y lo corrido de la vigencia 2025.

Nota: El establecimiento de este período no limita la facultad de la Oficina de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados

Limitaciones al Alcance: *Se describen en caso de existir*

4. CRITERIOS

- *Decreto Único Reglamentario del sector TIC 1078 de 2015*
- *Ley 1474 de 2011*
- *Ley 80 de 1993*
- *Ley 1712 de 2014*
- *Resolución 1519 de 2020*
- *Resolución 500 de 2021.*
- *Resolución 1978 de 2023.*

- *Decreto 612 de 2018*
- *Manual operativo de MIPG versión 6.*
- *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas versión 6.*
- *Políticas y Procedimientos internos de la Entidad.*

5. METODOLOGÍA

El presente ejercicio auditor se realizó en el marco de las Normas Internacionales de Auditoría Interna emitidas por el Instituto de Auditores Internos, el *"Estatuto de Auditoría de la Oficina de Control Interno del Ministerio de Minas y Energía"* y el *"Código de Ética de la Oficina de Control Interno del Ministerio de Minas y Energía"* aprobados por el Comité Institucional de Coordinación de Control Interno, así como los lineamientos establecidos para el Proceso Auditoria y Evaluación.

Planeación y desarrollo de la Auditoría:

En concordancia con lo definido en la Plan Anual de Auditoría, se realizó estimación y programación de la presente auditoría para ser realizada en el primer ciclo del año, adicionalmente en la fase de planeación se realizó una identificación preliminar del proceso a través del conocimiento de la unidad auditable, etapa en la que se conocieron aspectos relevantes de la gestión del proceso como son sus riesgos, planes y proyectos entre otra información publicada y disponible para consulta.

Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas por la auditora a cargo de la realización del trabajo. Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

Como última etapa, con la información identificada y consolidada a lo largo del presente trabajo se construye el informe cuyos resultados se clasifican en conclusiones, hallazgos, oportunidad de mejora y recomendaciones; cuyas definiciones se detallan a continuación:

- **Conclusiones**: Es el resumen de los aspectos principales analizados en el ejercicio auditor, los cuales están soportados en evidencias y pruebas realizadas.

- **Hallazgo:** Es el resultado de la comparación de La Condición (situación detectada o hechos identificados) con El Criterio que se refiere al deber ser (cumplimiento de normas, reglamentos, lineamientos o procedimientos). El hallazgo deben ser objeto de formulación de acciones tendientes a eliminar de fondo las causas que las originaron, las cuales harán parte del correspondiente plan de mejoramiento.

- **Oportunidad de mejora:** Situación que podría convertirse en un futuro incumplimiento de un requisito (hallazgo) o materialización de un riesgo que podría llegar a tener efectos sobre el cumplimiento de los objetivos, procesos, planes, programas o proyectos. En caso de que, producto de análisis realizado, el proceso determine que

se acogerán las oportunidades de mejora y se tomen medidas para su tratamiento o en caso de que sea requerido, las mismas deberán documentarse en el correspondiente plan de mejoramiento.

- **Recomendación:** Es una sugerencia encaminada a dar pautas para subsanar las causas identificadas en el ejercicio de auditoría realizado.

7. RESUMEN EJECUTIVO DE LOS RESULTADOS DE LA AUDITORIA

Tipo de Resultado	Consecutivo	Título	Proceso / Área Responsable	Plan de Mejoramiento	Componente de Control Interno que afecta	Dimensión MIPG que afecta
Hallazgo	H-01-2025	Incumplimiento de lineamientos del Modelo de Referencia de Arquitectura Empresarial.	Grupo de Trabajo de tecnología de la Información	Obligatorio	Ambiente de Control	Gestión con Valores para Resultados
Hallazgo	H-02-2025	Gestión de riesgos del proceso	Grupo de Trabajo de tecnología de la Información	Obligatorio	Evaluación del Riesgo	Gestión con Valores para Resultados Control Interno
Hallazgo	H-03-2025	Debilidades en la aplicación de Controles de Seguridad Física	Grupo de Trabajo de tecnología de la Información	Obligatorio	Actividades de Control	Gestión con Valores para Resultados
Hallazgo	H-04-2025	Incumplimiento de Acuerdos de Niveles de Servicio	Grupo de Trabajo de tecnología de la Información	Obligatorio	Actividades de Control Actividades de Monitoreo	Gestión con Valores para Resultados Evaluación de Resultados
Hallazgo	H-05-2025	Prestación de Servicios de soporte de Mesa de Ayuda Prestados sin Contrato Formal.	Grupo de Trabajo de tecnología de la Información	Obligatorio	Actividades de Control Actividades de Monitoreo	Direccionamiento Estratégico y Planeación Gestión con Valores para Resultados Evaluación de Resultados
Oportunidad de Mejoramiento	OM-01-2025	– Fecha de Publicación de Documentación en la página web	Grupo de Trabajo de tecnología de la Información	Voluntario	Información y Comunicación	Gestión con Valores para Resultados Información y Comunicación

Tipo de Resultado	Consecutivo	Título	Proceso / Área Responsable	Plan de Mejoramiento	Componente de Control Interno que afecta	Dimensión MIPG que afecta
			Y Grupo de Comunicación y Prensa			
Oportunidad de Mejoramiento	OM-02-2025	Publicación de Documentación del Proceso	Grupo de Trabajo de tecnología de la Información Y Oficina de Planeación y Gestión Internacional – Grupo de Gestión de Desempeño	Voluntario	Información y Comunicación	Información y Comunicación

8. RESULTADOS DETALLADOS DE LA AUDITORIA

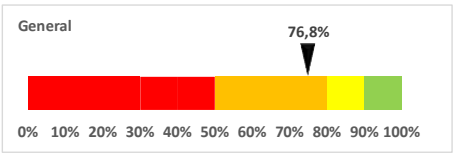
8.1. COMPONENTE AMBIENTE DE CONTROL

La verificación del presente componente se llevó a cabo sobre los lineamientos y directrices emitidas por el Ministerio de Minas y Energía, con la finalidad de identificar su eficiencia y aplicación, en lo relacionado con la gestión de Tecnologías de Información y las Comunicaciones de la Entidad y su adherencia con los lineamientos emitidos por MinTIC para la Gestión de Tecnología.

Código de Integridad y Política de Gestión del Riesgo

Como parte de las pruebas realizadas al presente componente se aplicó un instrumento de valoración el 19 de mayo de 2025, dirigido al equipo de la unidad auditable (46 colaboradores), con el propósito de hacer un diagnóstico de conocimiento en cuanto al código de integridad, obteniendo los siguientes resultados:

Resultado general nivel de conocimiento				
Aspecto evaluado	**Total muestra**	**Cantidad Repuestas**	**%**	**Resultaado**
Socialización del Código de Integridad	46	38	82,6%	Nivel aceptable
Conocimiento del Cófigo de Integridad	46	36	78,3%	Fortalecer
Correlación conceptos valores : Servicio, Excelencia, Trabajo colaborativo, Nuestra gente	46	32	69,6%	Fortalecer
Promedio	**46**	**35**	**76,8%**	Fortalecer



Fuente: Elaboración Propia.

Escala nivel de conocimiento: a) Menor o igual 50% "Implementar acción de mejora", b) Mayor a 50% y Menor 80% "Fortalecer", c) Mayor o igual a 80% y Menor a 90% "Nivel aceptable", d) Mayor o igual a 90% "Buen nivel"

Así las cosas, se concluye que de un total de 46 colaboradores de la unidad auditable (Grupo de Trabajo de Tecnología de la Información), el 82,6% es decir a 38 les fue socializado y el 78.3% conocen el código de integridad (36 colaboradores), de otro lado, al verificar el nivel de conocimiento de los valores enmarcados en el Código de Integridad "Servicio, Excelencia, Trabajo colaborativo, Nuestra gente", se observó que el 69,6%, es decir 32 colaboradores, tienen conocimiento en los aspectos asociados al código de integridad. De lo cual, si bien se tiene un buen comportamiento de los aspectos evaluados, se recomienda continuar fortaleciendo el conocimiento del Código de Integridad entre los colaboradores del Ministerio de Minas y Energía. Por lo que se recomienda, de manera articulada con la Subdirección de Talento Humano fortalecer las actividades de apropiación del Código de integridad en los colaboradores del Ministerio de Minas y Energía.

Compromiso de la línea Estratégica

Se evidenció que la Entidad ha dispuesto distintos recursos, mecanismos, políticas, entre otras, para disponer de un ambiente de control en materia de gestión de tecnología de información y comunicaciones las cuales se relacionan con:

1. Destinación de recursos para:

- "*Fortalecimiento de las Capacidades tecnológicas del Ministerio de Minas y energía para facilitar el uso, acceso y aprovechamiento de la información minero-energética a Nivel Nacional*" a través del proyecto identificado con código BPIN 2020011000126.
- "*Fortalecimiento de la capacidad del Ministerio de Minas y Energía para implementar de manera efectiva la política de gobierno digital Nacional*" a través del proyecto identificado con código BPIN 202400000000198.

2. Asignación de Talento Humano y definición políticas para la gestión de Tecnologías de la Información y las Comunicaciones evidenciadas en los siguientes documentos:

- Asignación de funciones a fin de *"Proponer la adopción de políticas para el buen manejo y seguridad de la información sistematizada en el Ministerio, y promover el desarrollo e implementación de programas sistematizados"* a la Secretaría General mediante Decreto 030 de 2022.
- Definición de Grupo de trabajo y funciones para la gestión de Tecnologías de la Información y las Comunicaciones a través de la Resolución 631 de 2023.
- Adopción de las políticas aplicables al Modelo de Seguridad y Privacidad de la Información — MSPI del Ministerio de Minas y Energía, mediante resolución 40646 del primero de noviembre de 2023.

3. Articulación con la Planeación Institucional:

- Se observa que los planes (i)Plan estratégico de Tecnologías de la Información – PETI, (ii) Plan de tratamiento de riesgos de seguridad de la información y (iii) Plan de seguridad y privacidad de la información, fueron aprobados por el Comité Institucional de Gestión y Desempeño en concordancia con los lineamientos del decreto 612 de 2018.

Relación del proceso auditado con la implementación de habilitadores de "Arquitectura" y "Seguridad Digital" de las Políticas de Gobierno y Seguridad Digital.

Teniendo en cuenta que el objetivo del proceso de Gestión de Tecnologías de la Información y las Comunicaciones identificado en la caracterización se define como:

"Gestionar y optimizar los recursos de tecnología de información y comunicaciones como componentes claves para apoyar el cumplimiento de la misión institucional, facilitando el acceso, uso eficiente y aprovechamiento de las TIC´s"

Se identifica una relación directa del proceso con la aplicación de la política de gobierno digital y sus distintos componentes.

Es por esto que, en el desarrollo de la presente auditoría se evaluaron distintos aspectos relacionados con la implementación de los habilitadores transversales de Arquitectura y Seguridad Digital.

En línea con lo anterior, se identificó en primera instancia que el Ministerio de Minas y Energía ha definido un Plan Estratégico de Tecnologías de la Información – PETI, también ha adoptado políticas de seguridad y ha implementado el proceso de gestión de tecnologías de la información y las comunicaciones y lo ha incorporado en el mapa de procesos, con sus documentos descriptivos según los criterios adoptados por la entidad en su Sistema Integral de Gestión - SIG.

Particularmente en materia de Arquitectura, se verificaron los avances obtenidos respecto a la implementación del Modelo de Referencia de Arquitectura Empresarial evidenciando lo siguiente:

Ejercicios de Arquitectura Empresarial.

La Entidad desarrollo un ejercicio de arquitectura empresarial en la vigencia 2024 dentro del cual se definieron aspectos como la visión de arquitectura, el repositorio de Arquitectura empresarial y la hoja de ruta para la implementación de los diferentes dominios del MRAE, en concordancia con las disposiciones de Mintic.

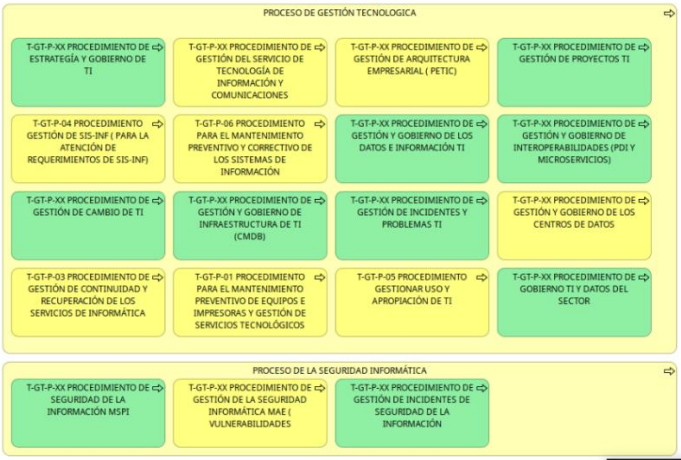
En este sentido revisado el archivo de Excel “Plan de Trabajo AE 2025”, de manera conjunta con el área auditada en sesión adelantada el pasado 7 de mayo de 2025 se identificó que se tiene una “hoja de ruta” en la que se identifican los procesos a abordar desde Arquitectura Empresarial dentro de la vigencia 2025, según se muestra a continuación:

Energía — HOJA DE RUTA AE

Proceso	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Proceso de gestión tecnológica.												
Proceso de seguridad informatica.												
Proceso de direccionamiento estratégico.												
Proceso de gestión del conocimiento, la información y la innovación.												
Proceso de minería.												
Proceso de energía.												
Proceso de hidrocarburos.												
Proceso socioambiental.												
Proceso de asuntos nucleares.												
Proceso de gestión documental.												
Proceso de gestión jurídica.												
Proceso de gestión contractual.												
Proceso de recursos físicos.												
Proceso de gestión financiera.												
Proceso de relacionamiento con grupos de valor.												
Proceso de talento humano.												
Proceso de gestión de comunicaciones.												
Proceso de Control Disciplinario.												
Proceso de mejoramiento.												
Proceso de evaluación independiente.												

Fuente: Plan de Trabajo AE 2025 aportado por el Grupo de TIC

Aunado a lo anterior, con el fin de identificar el avance en la construcción de artefactos y avance en la implementación de lineamientos del MRAE, se revisó el archivo de Excel “CATALOGO PROCESO TIC”, en el que se identifican los procedimientos que se han implementado y están en construcción en concordancia con los avances obtenidos y la hoja de ruta definida para la vigencia 2025, según se muestra a continuación:



Fuente: CATALOGO PROCESO TIC aportado por el Grupo de TIC

Tomando como base la imagen anterior se expuso por parte del área auditada que los procedimientos identificados con color “amarillo” ya fueron construidos y/o mejorados y se encuentran en proceso de formalización dentro del Sistema de Integrado de Gestión; por otra parte, los procedimientos identificados en color “verde” no se han construido.

Al respecto, es de anotar que, en particular, los procedimientos de “Gestión de cambios” y “Disposición de residuos tecnológicos”, se encuentran directamente relacionados con el cumplimiento de los siguientes lineamientos de del MAE.

En este sentido se observa incumplimiento de los lineamientos

MGGTI.LI.GO.04 - Gestión de cambios - “La dirección de tecnologías y Sistemas de la información o quien haga sus veces debe definir e implementar formalmente un procedimiento de control de cambios”.

“MGGTI.LI.ST.12 Disposición de residuos tecnológicos. *La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, siguiendo las directrices de las áreas administrativas debe gestionar la correcta disposición de residuos tecnológicos de acuerdo con el Plan Institucional de Gestión Ambiental y teniendo en cuenta los lineamientos técnicos con los que cuente el gobierno nacional”.*

Respecto a este requisito, es importante tener en cuenta que el “Procedimiento de disposición de residuos tecnológicos”, es una de las evidencias de la implementación del lineamiento MGGTI.LI.ST.12. (**ver hallazgo No.1**)

Así las cosas, se evidencia que no se han implementado el 100% de los lineamientos del MRAE cuyo plazo de implementación aplicable para las Entidades del Orden Nacional y en particular para los Ministerios fue de 23 meses contados a partir de la expedición de la Resolución 1978 del 26 de mayo de 2023, esto es, hasta el mes de abril de 2025. (**Ver hallazgo No. 1**)

En adición a lo anterior, se identificó dentro del archivo “Plan de Trabajo AE 2025”, el siguiente cuadro con la relación de procedimientos por cada proceso de la Entidad, en la que se identificaron 19 procedimientos (8 Existentes y 11 Nuevos) según se muestra a continuación:

CÓDIGO	PROCEDIMIENTOS	AÑO	estado	ÁREAS
T-GT-P-XX	Procedimiento gestión del **arquitectura empresarial.**	2024	Existente	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento gestión de **planes y proyectos de TI - MGPTI**	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-04	Procedimiento gestión de **sistemas de información.**	2024	Existente	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-06	Procedimiento gestión de **mantenimiento de los sistemas de información.**	2025	Existente	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de gestión y gobierno de los **datos e información** de TI.	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de gestión y gobierno de **interoperabilidades** (PDI y Microservicios).	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento gestión del **servicio de tecnología** de información y comunicaciones.	2025	Existente	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de gestión y gobierno de **infraestructura** de TI (CMDB).	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de **gestión de cambio** de TI.	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de **gestión de incidentes y problemas** de TI.	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-03	Procedimiento gestión de la **continuidad**.	2025	Existente	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-01	Procedimiento para el **mantenimiento preventivo de equipos e impresoras y gestión de servicios tecnológicos**.	2025	Existente	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de **Gobierno TI y Datos Sectorial.**	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-05	Procedimiento gestionar **uso y apropiación de TI.**	2024	Existente	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de **seguridad de la información MSPI.**	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-02	Procedimiento gestión de la **seguridad informática MAE.**	2025	Existente	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de gestión de **incidentes de seguridad** de la información **MSPI - CSIRT**	2025	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de **gestión y gobierno de estrategia TI** (MGGTI) (Seguimiento de todos los procedimientos, Apoyo en mesas de trabajo en Acuedos Marco Precios TICS)	2026	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones
T-GT-P-XX	Procedimiento de **gestión y gobierno de los centros de datos**	2027	Nuevo	Grupo de Tecnologías de la Información y las Comunicaciones

Fuente: Plan de Trabajo AE 2025 aportado por el Grupo de TIC

Sin embargo, verificado el repositorio publicado en el SIG se identificaron 6 procedimientos, según la imagen a continuación:

Fuente: Página Web de la Entidad

En este sentido se recomienda adelantar los tramites de formalización y publicación de los procedimientos existentes a fin de asegurar su implementación y aplicación al interior de la Entidad.

HALLAZGO Nº 1 - Incumplimiento de lineamientos del Modelo de Referencia de Arquitectura Empresarial.

Condición:

Se identificó en primera instancia que el Ministerio de Minas y Energía ha adoptado políticas de seguridad y ha implementado el proceso de gestión de tecnologías de la información y las comunicaciones y lo ha incorporado en el mapa de procesos, con sus documentos descriptivos según los criterios adoptados por la entidad en su Sistema Integral de Gestión - SIG.

No obstante, lo anterior, se evidenció en la revisión documental del SIG que los procedimientos de "Gestión de cambios" y "Disposición de residuos tecnológicos", no se encuentran documentados dentro del proceso, lo cual fue confirmado por parte del área auditada mediante correo electrónico del 28 de abril de 2025.

En este sentido se evidenció que, no se han implementado el 100% de los lineamientos del MRAE cuyo plazo de implementación aplicable para las Entidades del Orden Nacional y en particular para los Ministerios fue de 23 meses contados a partir de la expedición de la Resolución 1978 del 26 de Mayo de 2023, esto es, hasta el mes de Abril de 2025.

Criterio(s):

Resolución 1978 de 2023 *"Por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones"*

Artículo 4°. Marco de Referencia de Arquitectura Empresarial. *Los sujetos obligados deberán adoptar el Marco de Arquitectura Empresarial,* para *lo cual deberán dar cumplimiento a los lineamientos contenidos en el documento "MRAE.DM - DOCUMENTO MAESTRO", correspondiente al Anexo 1 de la presente resolución, y que hace parte integral de la misma.*

"Artículo 5°. Plazos para la implementación del Marco de Referencia de Arquitectura Empresarial. *Los sujetos obligados deberán implementar las actividades establecidas en la presente Resolución dentro de los siguientes plazos, que serán contados a partir de su entrada en vigencia.*

5.1 Entidades del orden nacional:

Grupo de entidades (según naturaleza jurídica)	*Bloque 1: 40% de lineamientos.*	*Bloque 2: 70% de lineamientos*	*Bloque 3: 100% de lineamientos*
Departamentos Administrativos, Ministerios, Empresas Industriales y Comerciales del Estado, Sociedades de Economía Mixta, Institutos Científicos y Tecnológicos	***10 meses***	***17 meses***	***23 meses***
Unidades Administrativas Especiales, Superintendencias, Agencias Estatales de Naturaleza Especial, Establecimientos Públicos, Empresas de Servicios Públicos	*11 meses*	*18 meses*	*25 meses*
Empresas Sociales del Estado, Entidades de Naturaleza Jurídica Especial, otras Entidades de la Rama Ejecutiva	*12 meses*	*20 meses*	*27 meses*

"(negrita fuera de texto)

Modelo de Gestión Y gobierno de TI, lineamientos MGGTI.LI.GO.04 y MGGTI.LI.ST.12

"MGGTI.LI.GO.04 - Gestión de cambios - "La dirección de tecnologías y Sistemas de la información o quien haga sus veces debe definir e implementar formalmente un procedimiento de control de cambios."

"MGGTI.LI.ST.12 Disposición de residuos tecnológicos

La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, siguiendo las directrices de las áreas administrativas debe gestionar la correcta disposición de residuos tecnológicos de acuerdo con el Plan Institucional de Gestión Ambiental y teniendo en cuenta los lineamientos técnicos con los que cuente el gobierno nacional"

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Debilidades en la adopción del Modelo de Referencia de Arquitectura Empresarial y del Modelo de Gestión y Gobierno de TI.
- Falta de adopción de buenas prácticas de gestión de Tecnología.
- Debilidad en la apropiación de conocimientos y habilidades para la implementación de la política de gobierno digital y sus componentes.
- Debilidad en el seguimiento y control de tiempos de implementación del MRAE en concordancia con la Resolución 1978 de 2023.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- Inadecuado tratamiento de riesgos tecnológicos y de seguridad de la información relacionados con la implementación y cambios de sistemas de información y elementos de infraestructura tecnológica.
- Posible afectación reputacional por incumplimiento de disposiciones legales de la resolución 1978 de 2023.

Recomendación(nes) específica(s):

- Aplicar evaluaciones del modelo de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI así como del Modelo de Referencia de Arquitectura Empresarial y sus componentes.
- Adoptar las recomendaciones de la guía MGGTI.G.GO - GOBIERNO DE TI del Modelo de Gestión y Gobierno de TI.
- Adelantar los tramites internos de formalización de procedimientos dentro del SIG, de manera articulada con la OPGI.

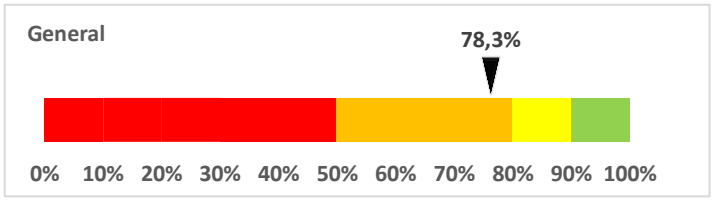
8.2 COMPONENTE EVALUACIÓN DEL RIESGO

Para este componente se llevó a cabo el análisis del riesgo de gestión a cargo del Grupo de Trabajo de Tecnología, asimismo se realizó evaluación en cuanto al diseño y ejecución de los controles de los riesgos identificados, de conformidad con la información suministrada por la dependencia auditada.

Nivel de Conocimiento y aprehensión en materia de Gestión de Riesgos

Como parte de las pruebas realizadas al presente componente se aplicó un instrumento de valoración el 19 de mayo 2025, dirigido al equipo de la unidad auditable (46 colaboradores), con el propósito de hacer un diagnóstico de conocimiento en cuanto al conocimiento en materia de gestión de riesgos, obteniendo los siguientes resultados:

Resultado general nivel de conocimiento				
Aspecto evaluado	**Total muestra**	**Cantidad Repuestas**	**%**	**Resultado / Mejoramiento**
Política de gestión de riesgos del MME	46	44	95,7%	Buen nivel
Beneficios de la gestión de riesgos	46	33	71,7%	Fortalecer
Conflicto de interés real	46	31	67,4%	Fortalecer
Promedio	**46**	**36**	**78,3%**	Fortalecer



Fuente: Elaboración Propia.

Escala nivel de conocimiento: a) Menor o igual 50% “Implementar acción de mejora”, b) Mayor a 50% y Menor 80% “Fortalecer”, c) Mayor o igual a 80% y Menor a 90% “Nivel aceptable”, d) Mayor o igual a 90% “Buen nivel”

De la ilustración anterior, se concluye que de un total de 46 colaboradores de la unidad auditable (Grupo de Trabajo de Tecnología), el 95.7% es decir 44 conocen la política de gestión del riesgo y el 71.7% (33 colaboradores), identifican los beneficios de la gestión del riesgo en la Entidad, de otro lado, al verificar el nivel del conocimiento en cuanto al conflicto de interés, se observó que el 67.4% (31 colaboradores) saben en qué consiste el conflicto de interés y tienen claridad de ello. Por cuanto, se recomienda dar continuidad a las acciones

que desde la Segunda línea (Oficina de Planeación y Gestión Internacional) se desarrollan en el marco la gestión de riesgos de la Entidad.

Gestión de Riesgos del Grupo TIC

Se identificó en primera instancia que el proceso de Gestión de Tecnologías de Ia Información y las Comunicaciones identifica, analiza, evalúa, realiza el seguimiento y deseña y aplica controles en concordancia con los lineamientos del Manual de Gestión de Riesgos de la Entidad, identificado con código E-ME-M-02 V4 del 26 de diciembre de 2024.

A partir de lo anterior, teniendo en cuenta la última actualización del Manual de Gestión de Riesgos, se identificó que para la vigencia 2025 se mantuvo la misma identificación de riesgos de gestión (4 riesgos) y de corrupción (2 riesgos) que habían sido identificados en la vigencia 2024, sin embargo, a nivel de seguridad de la información se identificaron 4 riesgos diferentes, por lo tanto, se presentan a continuación los resultados de la evaluación de la gestión de riesgos realizada.

Análisis de Riesgos de seguridad de la información.

Respecto a la identificación de Riesgos de Seguridad de la Información, es importante prever los lineamientos dados por la Guía de Administración del Riesgo y Diseño de Controles emitida por el DAFP y el Documento Maestro del Modelo de Seguridad y Privacidad de la Información; así como, el Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en Entidades Públicas emitidos por MinTIC, en lo relacionado con la identificación de los activos de información como etapa prevista a la identificación de riesgos.

A partir de lo anterior, en concordancia con las disposiciones de la ley 1712 de 2014 y la resolución 1519 de 2020, se realizó verificación del inventario de activos de información, publicado en la sección de transparencia de la página web de la Entidad, el cual puede ser consultado en el siguiente link:

https://www.minenergia.gov.co/es/servicio-al-ciudadano/gestion-documental/instrumentos-de-gesti%C3%B3n-de-la-informaci%C3%B3n/

Fuente: Página Web de la Entidad

A partir de lo anterior se identificaron 1847 de los cuales 21 corresponden a la tipología de Software y 1826 se identificaron como Información (alineados con las Tablas de Retención Documental).

En este sentido, se observa en primera instancia que no se tienen identificados activos asociados a tipologías como servicios, personas, hardware, instalaciones, servicios, entre otros, aplicables al contexto de la Entidad.

Situación que incumple el numeral 3.1.6 Identificación de activos de información, paso 3 del el cual establece:

"Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, (...)". ***(Ver Hallazgo No.2)***

A partir de lo anterior se verificó la matriz de riesgos del proceso evidenciando que, para la vigencia 2025 se identificaron 4 riesgos de seguridad de la información en la matriz de riesgos definida por la Entidad, en la cual se evidenció la descripción, identificación de causas, análisis de probabilidad e impacto, entre otros aspectos relativos a la identificación análisis y evaluación de los riesgos según se muestra a continuación:

Referencia	Proceso	Tipo de Riesgo	Descripción del Riesgo	Impacto	Causa o circunstancia Inmediata ¿Cómo?	Causa Raiz ¿Por a que?	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad anual	Probabilidad Inherente	%	Impacto	Observación de criterio	Impacto Inherente	%	Zona de Riesgo Inherente
1	GESTIÓN TECNOLÓGICA	Gestion	Posibilidad de afectacioneconómico y reputacional por o para Desarrollo de aplicaciones y sistemas sin cumplir con estándares de seguridad, permitiendo la introducción de vulnerabilidades explotables. debido a Falta de implementación de la metodología de desarrollo seguro y ausencia de mecanismos estrictos de control en la fase de codificación.	económico y reputacional	Desarrollo de aplicaciones y sistemas sin cumplir con estándares de seguridad, permitiendo la introducción de vulnerabilidades explotables.	Falta de implementación de la metodología de desarrollo seguro y ausencia de mecanismos estrictos de control en la fase de codificación.	Fallas Tecnologicas	4	Baja	40%	Entre 50 y 100 SMLMV	Entre 50 y 100 SMLMV	Moderado	60%	Moderado
2	GESTIÓN TECNOLÓGICA	Gestion	Posibilidad de afectacioneconómico y reputacional por o para Ausencia de supervisión continua de registros de actividad en los sistemas de información, permitiendo que incidentes de seguridad pasen desapercibidos. debido a Falta de un procedimiento estandarizado para la gestión y análisis de logs de seguridad, junto con la ausencia de herramientas automatizadas de monitoreo y alerta.	económico y reputacional	Ausencia de supervisión continua de registros de actividad en los sistemas de información, permitiendo que incidentes de seguridad pasen	Falta de un procedimiento estandarizado para la gestión y análisis de logs de seguridad, junto con la ausencia de herramientas automatizadas de monitoreo	Ejecucion y Administracion de procesos	4	Baja	40%	Entre 100 y 500 SMLMV	Entre 100 y 500 SMLMV	Mayor	80%	Alto
4	GESTIÓN TECNOLÓGICA	Gestion	Posibilidad de afectacioneconómico y reputacional por o para Pérdida de información crítica debido a fallos en los procesos de respaldo, almacenamiento y recuperación de datos, afectando la continuidad operativa del ministerio. debido a Ausencia de un proceso estructurado de respaldo de información y monitoreo de la efectividad de los backups.	económico y reputacional	[illegible] crítica debido a fallos en los procesos de respaldo, almacenamiento y recuperación de datos, afectando la continuidad	Ausencia de un proceso estructurado de respaldo de información y monitoreo de la efectividad de los backups.	Fallas Tecnologicas	4	Baja	40%	Entre 100 y 500 SMLMV	Entre 100 y 500 SMLMV	Mayor	80%	Alto
5	GESTIÓN TECNOLÓGICA	Gestion	Posibilidad de afectacioneconómico y reputacional por o para Desactualización en la clasificación de activos de información, lo que impide definir estrategias efectivas de continuidad del negocio y recuperación ante incidentes. debido a Falta de un proceso de actualización periódica de la clasificación de información y de integración con la gestión de continuidad del negocio.	económico y reputacional	Desactualización en la clasificación de activos de información, lo que impide definir estrategias efectivas de continuidad del negocio y recuperación ante	Falta de un proceso de actualización periódica de la clasificación de información y de integración con la gestión de continuidad del negocio.	Ejecucion y Administracion de procesos	4	Baja	40%	Mayor a 500 SMLMV	Mayor a 500 SMLMV	Catastrófico	100%	Extremo

Fuente: Matriz de riesgos del Proceso de Gestión TIC.

Sin embargo, no se evidenció que se realice actualmente la identificación de amenazas y vulnerabilidades, ni se relacionan los grupos de activos de manera concordante con los identificados en el inventario de activos de información, lo cual fue confirmado en sesión del pasado 15 de mayo de 2025.

Lo anterior en contravía de lo dispuesto por el numeral 3.1.7 Modelo Nacional de Gestión de Riesgos de Seguridad Digital según se cita a continuación.

"3.1.7 Identificar los riesgos inherentes de seguridad de la información

Como lo indica el Paso 2 de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas" emitida

por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- *Pérdida de la confidencialidad*
- *Pérdida de la integridad*
- *Pérdida de la disponibilidad*

(...) ***Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.*** *(...)" **(negrita fuera de texto)**.*
(Ver Hallazgo No. 2)

Análisis de Riesgos de Corrupción.

Se evidenció que para la vigencia 2025 se identificaron 2 riesgos de corrupción en la matriz de riesgos definida por la Entidad, en la cual se evidenció la descripción, identificación de causas, análisis de probabilidad e impacto, entre otros aspectos relativos a la identificación análisis y evaluación de los riesgos según se muestra a continuación:

Referencia	Proceso	Descripción del Riesgo	Causa Inmediata ¿Cómo se podria dar la corrupción?	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad anual	Probabilidad Inherente	%	Impacto Inherente	Zona de Riesgo Inherente	No. Control	Descripción del Control	Cargo del reponsable del control	Acción que realiza
2	GESTIÓN TECNOLÓGICA	Posibilidad de recibir cualquier dádiva o beneficio a nombre propio o de terceros por Entrega de incentivos, regalos o favores personales a funcionarios para direccionar contratos de adquisición o desarrollo de software, comprometiendo la transparencia del proceso.	Entrega de incentivos, regalos o favores personales a funcionarios para direccionar contratos de adquisición o desarrollo de software, comprometiendo la transparencia del proceso.	Fraude Interno	4	Baja	40%	Catastrófico	Extremo	1	El funcionario TIC, realiza un seguimiento a los desarrollos adquiridos o a las adquisiones registradas para verificar que estén acordes con las necesidades planetadas por la entidad	Funcionario TIC	Identificar y realizar seguimiento a las necesidades de soluciones y desarrollos de software
3	GESTIÓN TECNOLÓGICA	Posibilidad de recibir cualquier dádiva o beneficio a nombre propio o de terceros por Incorporación de funciones ocultas, puertas traseras o vulnerabilidades en el código fuente de soluciones Open Source desarrolladas internamente, con el fin de obtener acceso privilegiado o control indebido sobre los sistemas.	Incorporación de funciones ocultas, puertas traseras o vulnerabilidades en el código fuente de soluciones Open Source desarrolladas internamente, con el fin de obtener acceso privilegiado o control indebido sobre los sistemas.	Fraude Interno	4	Baja	40%	Catastrófico	Extremo	1	El funcionario TIC realiza revisiones de códigos y trazabilidad de auditoria en los repositorios opensource, igualmente, valida que se realice la gestión de versiones	Funcionario TIC	1. Implementar revisiones de código colaborativas (Code Reviews) con trazabilidad y auditoria de cambios en los repositorios Open Source. 2. Supervisar cada contribución al código mediante sistemas de gestión de versiones (Git, commits firmados y auditoria de merges).

Fuente: Matriz de riesgos del Proceso de Gestión TIC.

Al respecto es importante observar que no se detecta una relación directa entre el control aplicado y el riesgo identificado toda vez que no se identifica la manera en la que el control:

"El funcionario TIC, realiza un seguimiento a los desarrollos adquiridos o a las adquisiones registradas para verificar que estén acordes con las necesidades planetadas por la entidad"

Mitigue el riesgo de:

"Posibilidad de recibir cualquier dádiva o beneficio a nombre propio o de terceros por Entrega de incentivos, regalos o favores personales a funcionarios para direccionar contratos de adquisición o desarrollo de software, comprometiendo la transparencia del proceso."

Adicionalmente, teniendo en cuenta que la causa asociada al riesgo se registra en la matriz de la siguiente manera:

*"**Entrega de incentivos, regalos o favores personales a funcionarios** para direccionar contratos de adquisición o desarrollo de software, comprometiendo la transparencia del proceso." **(negrita fuera de texto).***

No se identifica que, en los atributos de diseño de control, se haya contemplado la identificación del propósito del mismo de manera que *"indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo"* en concordancia con los lineamientos dados por la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4, emitida por el DAFP. **(Ver Hallazgo No. 2)**

De otra parte, se observa en la matriz se han definido los siguientes parámetros para la valoración de controles.

Evaluación del riesgo - Valoración de los controles												
						Atributos						
No. Control	Descripción del Control	Cargo del reponsable del control	Acción que realiza	Evidencia esperada del control	Afectación	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia
1	El funcionario TIC, realiza un seguimiento a los desarrollos adquiridos o a las adquisiones registradas para verificar que estén acordes con las necesidades planetadas por la entidad	Funcionario TIC	Identificar y realizar seguimiento a las necesidades de soluciones y desarrollos de software	informes consolidados de avances de desarrollo	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro

Fuente: Matriz de riesgos del Proceso de Gestión TIC.

De otra parte, aunque se evalúa el control como "documentado", *no se referencia el procedimiento, manual instructivo, política u otros aplicables en donde se establece la manera en la que se ejecuta, es decir que no se establece el "como"* se realiza la actividad de control ni se indica la manera en que se gestionan las desviaciones que puedan presentarse en la ejecución del control; lo que conlleva el desconocimiento de los pasos 4 y 5 del numeral *"3.2.2 Valoración de los controles – diseño de controles"* de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4, la cual establece:

"3.2.2 Valoración de los controles – diseño de controles

Paso 4 Debe establecer el cómo se realiza la actividad de control. Paso 5 Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control."

Monitoreo de Riesgos,

Se evidenció que el proceso de Gestión TIC realiza monitoreo periódico de los riesgos a su cargo y reporta las evidencias en concordancia con los lineamientos dados por la Oficina de Planeación y Gestión Internacional - OPGI.

Los soportes del monitoreo realizado fueron consultados en los siguientes enlaces

Vigencia 2024
https://minenergiacol-my.sharepoint.com/personal/ajpena_minenergia_gov_co/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fajpena%5Fminenergia%5Fgov%5Fco%2FDocuments%2FSGC%20MINENERG%C3%8DA%202023%2FGesti%C3%B3n%20de%20riesgos%20y%20oportunidades%2FRiesgos%202024%2FMatrices%5Fpor%5FProceso%2FGesti%C3%B3n%5FTecnol%C3%B3gica%2FGesti%C3%B3n&ct=1747757765113&or=Teams%2DHL&ga=1&LOF=1

Vigencia 2025

https://minenergiacol-my.sharepoint.com/personal/ajpena_minenergia_gov_co/_layouts/15/onedrive.aspx?ct=1747250085292&or=OWA%2DNT%2DMail&ga=1&id=%2Fpersonal%2Fajpena%5Fminenergia%5Fgov%5Fco%2FDocuments%2FSGC%20MINENERG%C3%8DA%202023%2FGesti%C3%B3n%20de%20riesgos%20y%20oportunidades%2FRiesgos%202025%2FMatrices%5Fpor%5Fproceso%2FGesti%C3%B3n%5FTecnol%C3%B3gica&xsdata=MDV8MDJ8fDA4NjYzYmMxOTRiOTRhMDhjNDU5MDhkZDkzMWJiM2VmfGQ4MjYzNmJlNmRkMjRlNjRhMjg0N2EzNDAyZjI0ZTI3fDB8MHw2Mzg4Mjg0NjkzNDg3MTM1NjF8VW5rbm93bnxWR1ZoYlhOVFpXTjFjbWwwZVZOObGNuWnBZMlY4ZXlKV0lqb2lNQzR3TGpBd01EQWlMQ0pRSWpvaVYybHVNeklpTENKQlRpSTZJazkwYUdWeUlpd2lWMVFpT2pFeGZRPT18MXxMMk5vWVhSekx6RTVPbTFsWlhScGJtZGZXbTFhYkU5WFZYaE5SMDEwVFZSUk1VNURNREJOTWtwb1RGUnNiVTVFWTNST2JVazBUVVJKTWxsWFJtbFBSR014UUhSb2NtVmhaQzUyTWk5dFpYTnpZV2RsY3k4eE56UTNNalV3TVRNME1qY3h8YTcwNDgyZDVjY2UwNDZhZmM0NTkwOGRkOTMxYmIzZWZ8ZmJhNmM1MGI1MzAxNDczNDgzOWQ0MzUzYzI1MTlhZTg%3D&sdata=bmRtbWhJVTdETWNTS1AvbmUxbjRBR1ZrcW1zZGxtSmIreWlPaUR1dXJqaz0%3D&ovuser=d82636be%2D6dd2%2D4e64%2Da284%2D7a3402f24e27%2Cravaca%40minenergia%2Egov%2Eco&OR=Teams%2DHL&CT=1747757946906&clickparams=eyJBcHBOYW1lIjoiVGVhbXMtRGVza3RvcCIsIkFwcFZlcnNpb24iOiIxNDE1LzI1MDQxNzE5MzExIiwiSGFzRmVkZXJhdGVkVXNlciI6ZmFsc2V9

A partir de lo anterior se realizó verificación de los siguientes reportes de monitoreo:

Para el monitoreo del riesgo:

"Posibilidad de afectación económico y reputacional por Retrasos en la ejecución presupuestal, sobrecostos y afectación en la continuidad operativa debido a Ausencia de un mecanismo de planeación estratégica que permita programar con antelación las necesidades tecnológicas y optimizar la ejecución del presupuesto TIC".

Se identificó como causa:
"Retrasos en la ejecución presupuestal, sobrecostos y afectación en la continuidad operativa"

Identificación del riesgo									Análisis del riesgo inherente						
Referencia	Proceso	Tipo de Riesgo	Descripción del Riesgo	Impacto	Causa o circunstancia Inmediata ¿Cómo?	Causa Raiz ¿Por a que?	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad anual	Probabilidad Inherente	%	Impacto	Observación de criterio	Impacto Inherente	%	Zona de Riesgo Inherente
11	GESTIÓN TECNOLÓGICA	Gestión	Posibilidad de afectacion económico y reputacional por Retrasos en la ejecución presupuestal, sobrecostos y afectación en la continuidad operativa debido a Ausencia de un mecanismo de planeación estratégica que permita programar con antelación las necesidades tecnológicas y optimizar la ejecución del presupuesto TIC.	económico y reputacional	Retrasos en la ejecución presupuestal, sobrecostos y afectación en la continuidad operativa	Ausencia de un mecanismo de planeación estratégica que permita programar con antelación las necesidades tecnológicas y optimizar la ejecución del presupuesto TIC.	Ejecucion y Administracion de procesos	2	Muy Baja	20%	Entre 100 y 500 SMLMV	Entre 100 y 500 SMLMV	Mayor	80%	Alto

Fuente: Matriz de riesgos del Proceso de Gestión TIC.

No obstante lo anterior y según se evidenció en sesión de auditoría de verificación de la operación de Mesa de Ayuda, que el contrato GGC- 643- 2024, suscrito con el proveedor B2B TIC cuyo objeto fue:

"Objeto Contractual: *Prestar los servicios de Mesa de Ayuda para la atención de requerimientos de la infraestructura TIC de usuarios finales para el MNE, lo cual comprende el mantenimiento preventivo y correctivo con suministro de repuestos"*

Venció el pasado 31 de diciembre de 2024 y a la fecha de la auditoría (mes de mayo de 2025) aun no se había suscrito, situación tal que evidencia desviaciones en la aplicación del control**. (Ver hallazgo 2)**

Al respecto, teniendo en cuenta que para el primer trimestre de 2025 no se reportó materialización del riesgo y que a nivel de tratamiento de riesgo se definió como control:

"El funcionario del Grupo TICs, verifica que se realice el cumplimiento del cronograma anual de contrataciones TIC, que este se encuentre actualizado para que garantice la optimización del presupuesto y la oportunidad en las compras; adicionalmente, realiza control y seguimiento a los contratos TIC suscritos"

Se verificó el cronograma definido en el cual se realiza el seguimiento del proceso contractual según se muestra en la imagen a continuación:

PRIORIDAD	OBJETO	FECHA DE VENCIMIENTO O RENOVACIÓN	PRESUPUESTO	IMPACTO PRESUPUESTAL EN EL PROYECTO	INICIO ESTRUCTURACIÓN DOCUMENTOS	ENTREGA ABOGADA TIC DOCUMENTOS PARA SOLICITUD DE COTIZACIÓN	REVISIÓN DE DOCUMENTOS PARA SOLICITUD DE COTIZACIÓN	SOLICITUD A FINANCIERA - FORMATO SOLICITUD DE COTIZACIÓN	CONSOLIDACIÓN DOCUMENTOS SOLICITUD DE COTIZACIÓN	RADICACIÓN A CONTRATACIÓN SOLICITUD DE COTIZACIÓN	TIEMPO CONTRATACIÓN DE REVISIÓN DE PUBLICACIÓN	TIEMPO DE EVENTO DE COTIZACIÓN	ENTREGA DEFINITIVA AJUSTES A ESTUDIO PREVIO TÉCNICO -	RADICACIÓN DEL ESTUDIO PREVIO A CONTRATACIÓN	TIEMPO DE PROCESO	FECHA ESTIMADA DE ADJUDICACIÓN	ESTADO
ALTA	Prestar servicios de atención de mesa de ayuda a usuario final e infraestructura TIC, incluido mantenimiento preventivo/correctivo y bolsa de suministro de respuestos, accesorios, servicios y equipos tecnologicos	31 DE DICIEMBRE/2024	$ 1.152.800.000	3,66%	24 DE FEBRERO AL 10 MARZO	10 DE MARZO	10 AL 17 DE MARZO	17 AL 19 DE MARZO	20 AL 21 DE MARZO	25 DE MARZO	25 AL 28 DE MARZO	10 DÍAS (03 AL 14 DE ABRIL)	15 AL 16 DE ABRIL	17 DE ABRIL	2 MESES	17 DE JUNIO	INICIANDO - AJUSTES SOLICITUD PROVEEDORES

Fuente: Cronograma de contrataciones TIC aportado por el Grupo de TIC dentro del monitoreo de riesgos.

De lo anterior se observa que la dependencia cuenta con un instrumento de control y documenta el seguimiento; sin embargo, el tratamiento definido no fue efectivo para garantizar *"la optimización del presupuesto y la oportunidad en las compras"*, toda vez que se proyecta adjudicar el proceso hasta el mes de junio según lo indicado en el reporte de

monitoreo del primer trimestre de 2025; esto es, aproximadamente 6 meses después de la finalización del último contrato de mesa de ayuda.

Finalmente, teniendo en cuenta que no se reportó la materialización del riesgo, se pone de presente que esta situación afecta el seguimiento y verificación de la eficacia de implementación de los controles que realiza la segunda línea defensa la cual se encarga de:

"supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos."

Según lo definido por el Manual Operativo de MIPG versión 6. séptima Dimensión – Control Interno

HALLAZGO Nº 2 - Gestión de riesgos del proceso

Condición:

Una vez revisada la gestión de riesgos adelantada por parte del Grupo de Trabajo de TIC se observaron los siguientes aspectos:

Riesgo	***Situación***
En General para los riesgos de seguridad de la Información	*No se evidenció que se realice actualmente la identificación de amenazas y vulnerabilidades, ni se relacionan los grupos de activos de información con el riesgo, lo cual fue confirmado por el área auditada en sesión del 15 de mayo de 2025, incumpliendo lo dispuesto por el numeral 3.1.7 Modelo Nacional de Gestión de Riesgos de Seguridad Digital.* *De otra parte, se observa que no se registran activos de tipos, hardware, servicio, personas, entre otros, en el inventario de activos de información de la Entidad, de conformidad con los dispuesto en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital*
Riesgo 2: "Posibilidad de recibir cualquier dádiva o beneficio a nombre propio o de terceros por Entrega de incentivos, regalos o favores personales a funcionarios para direccionar contratos de adquisición o	*No identifica que, en los atributos de diseño de control, se haya contemplado la identificación del propósito del mismo, de manera que "indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo", lo anterior d*

Riesgo	***Situación***
desarrollo de software, comprometiendo la transparencia del proceso."	*conformidad con los lineamientos dados por la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4, emitida por el DAFP.*
Riesgo 11. "Posibilidad de afectación económico y reputacional por Retrasos en la ejecución presupuestal, sobrecostos y afectación en la continuidad operativa debido a Ausencia de un mecanismo de planeación estratégica que permita programar con antelación las necesidades tecnológicas y optimizar la ejecución del presupuesto TIC."	Se evidenció en sesión de auditoría de verificación de la operación de Mesa de Ayuda, que el contrato GGC- 643- 2024, suscrito con el proveedor B2B TIC Venció el pasado 31 de diciembre de 2024 y a la fecha de la auditoría (mes de mayo de 2025) aún no se había suscrito, situación tal que evidencia desviaciones en la aplicación del control definido para la mitigación del riesgo de gestión. Adicionalmente teniendo en cuenta que no se reportó la materialización del riesgo, se pone de presente que esta situación afecta el seguimiento y verificación de la eficacia de implementación de los controles que realiza la segunda línea defensa la cual se encarga de: *"supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos."*

Fuente: Elaboración Propia.

Criterio(s):

1. ***Modelo nacional de Gestión de Riesgos de Seguridad de la Información.***

"3.1.6 Identificación de activos de información, paso 3"

"Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, (...)".

"3.1.7 Identificar los riesgos inherentes de seguridad de la información

Como lo indica el Paso 2 de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas" emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- *Pérdida de la confidencialidad*
- *Pérdida de la integridad*
- *Pérdida de la disponibilidad*

(...) Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. (...)" (negrita fuera de texto).

2. ***Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6***

"Valoración de los controles – diseño de controles

Tenga en cuenta para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes, por lo tanto se sugiere remitirse a dicho documento."

3. ***Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4***

"3.2.2 Valoración de los controles – diseño de controles

"Antes de valorar los controles es necesario conocer cómo se diseña un control, para lo cual daremos respuesta a las siguientes interrogantes: ¿Cómo defino o establezco un control para que en su diseño mitigue de manera adecuada el riesgo? Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

(...)
Paso 3 Debe indicar cuál es el propósito del control.
Paso 4 Debe establecer el cómo se realiza la actividad de control.
Paso 5 Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
(...)
"

4. ***Manual Operativo de MIPG versión 6. séptima Dimensión – Control Interno***

"(...) supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan

adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos. (...)"

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- *Debilidades en la adopción de lineamientos para la gestión de riesgo en entidades públicas.*
- *Debilidades metodológicas y falta de lineamientos por parte de la OPGI y Grupo TICS para el reporte de materialización de riesgos y alcance del monitoreo de los mismos en los riesgos de gestión, fiscales, de corrupción y /o de seguridad de la información.*
- *Debilidades en el diseño de Controles para mitigar los riesgos identificados.*
- *Posible falta de conocimiento y habilidades en materia de gestión del riesgo y diseño de controles por parte de la primera línea de defensa.*

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- *Posible incumplimiento de disposiciones legales, afectación de la operación y/o el logro de objetivos institucionales a partir de la materialización de riesgos no tratada.*
- *Posible afectación reputacional por la inadecuada gestión de riesgos por parte de la Entidad.*

Recomendación(nes) específica(s):

- ✓ *Evaluar la pertinencia de relacionar posibles casusas asociadas al riesgo corrupción de manera conjunta con la OPGI y fortalecer los controles y lineamientos para la gestión de riesgos y diseño de controles.*
- ✓ *Evaluar la pertinencia de incluir la descripción del propósito de los controles a fin de tener claramente identificadas las causas que mitigan, en concordancia con los lineamientos dados por la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 4, emitida por el DAFP.*
- ✓ *Fortalecer las habilidades y competencias del Grupo de Trabajo de Tecnología en materia de gestión de riesgos y diseño de controles.*

8.3 COMPONENTE ACTIVIDADES DE CONTROL

Con el objetivo de verificar las actividades de control del proceso, se inició revisando su operación procedimientos aplicables, en este sentido se realizaron las siguientes actividades

1. Visita al Data center (principal y alterno)
2. Operación de la Mesa de Ayuda

1. Vista al Data Center Principal y alterno

En concordancia con lo informado por el área auditada, la Entidad cuenta con un data center ubicado en la sede principal del Ministerio de Minas y Energía y un data center alterno, ubicado en el municipio de Soacha.

En visita realizada el día 11 de abril de 2025 al Data Center principal, se evidenció que se aplican controles de acceso físico desde el ingreso al edificio hasta el centro de datos, consistentes en la disposición de torniquetes y validación de permisos de acceso al edificio, circuito cerrado de televisión dentro del edificio, diligenciamiento de planillas de registro de acceso, acceso con tarjeta electrónica y adicionalmente se cuenta con un circuito cerrado de televisión (sistema de cámaras), el cual permite monitorear las actividades que se desarrollen dentro del Centro de Datos.

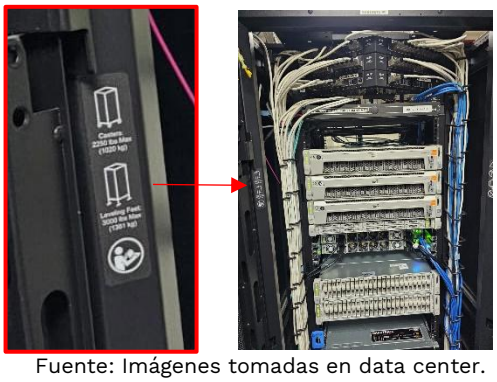
De otra parte, se realizó verificación de las condiciones medio ambientales y de instalación de equipos y cableado estructural evidenciando las siguientes situaciones:

1. Condiciones estructurales

   Se evidenció agrietamiento/fractura en una de las paredes del centro de datos tanto a nivel horizontal (a nivel del techo) como vertical, según se observa en las siguientes imágenes:

Fuente: Imágenes tomadas en data center.

Lo anterior representa condiciones de peligro para la vida de los colaboradores del Ministerio, la integridad física no solo del centro de datos sino del edificio y la integridad de los equipos y su operación, máxime teniendo en cuenta que los racks en los cuales se disponen los equipos están diseñados para soportar cargas de 1.020 Kilogramos, según se observa en la imagen a continuación:



Fuente: Imágenes tomadas en data center.

Adicionalmente, se identificaron sistemas de sujeción (chazos y tornillos) de las bandejas, ductos y escalerillas de cableado con condiciones de degaste (anclaje en techo agrietado, oxidación, tornillos sueltos), según se observa en las siguientes imágenes.

Fuente: Imágenes tomadas en data center.

Las cuales representan condiciones inseguras para el personal que atiende labores de mantenimiento dentro del data center, así como riesgos a la integridad del cableado estructurado del centro de datos.

De otra parte, se evidenciaron paredes perforadas sin conservar condiciones de impermeabilización y hermetismo dentro del data center lo que afecta potencialmente la conservación de las condiciones de temperatura y humedad del centro de datos, según se observa en las siguientes imágenes:

Fuente: Imágenes tomadas en data center.

También se identificó la presencia de elementos inflamables dentro de los racks, según se muestra a continuación:

Fuente: Imágenes tomadas en data center.

Lo anterior evidencia debilidades en la aplicación del control "A.11.2.1 Ubicación y protección de los equipos", del Modelo de Seguridad y Privacidad de la Información y del Anexo A. de la Norma ISO 27001, el cual establece:

> "A.11.2.1 Ubicación y protección de los equipos. Los equipos deben estar ubicados, y protegidos para reducir los riesgos de amenazas, peligros ambientales y las posibilidades de acceso no autorizado." **(Ver Hallazgo No. 3)**

Así las cosas, se recomienda monitorear constantemente el estado de la infraestructura física del edificio y del datacenter, evaluar la capacidad estructural de peso por metro cuadrado que soporta la zona en la que se ubica el data center y fortalecer los controles asociados a la operación e instalación de equipos en el data center principal.

De igual manera se recomienda evaluar la pertinencia de considerar ubicaciones alternas para la disposición de equipos del datacenter principal.

Data Center Alterno

Respecto al datacenter alterno se identificó que se encuentra ubicado en el municipio de Soacha y adicionalmente se evidenció que se localiza al lado de una polvorería situación que genera riesgos potenciales al complejo en el que se ubica el data Center.

Fuente: Imágenes tomadas en data center alterno.

De otra parte, se identificó que el sistema de aire acondicionado provisto en el data center alterno se encuentra alarmado, sin que se pudiera verificar sus condiciones de operación y mantenimiento, toda vez que no son de propiedad del ministerio; en este sentido según lo informado por el área auditada, se requirió implementar como contingencia un aire acondicionado portátil, como se observa en la imagen a continuación:

Fuente: Imágenes tomadas en data center alterno.

Así las cosas, se evidencian condiciones de riesgo para la operación del datacenter alterno del Ministerio, lo cual evidencia debilidades en la operación de los controles "A.17.2.1 Disponibilidad de instalaciones de procesamiento de información" y "*A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información"* del MSPI y el anexo A de la Norma ISO 27001 los cuales establecen:

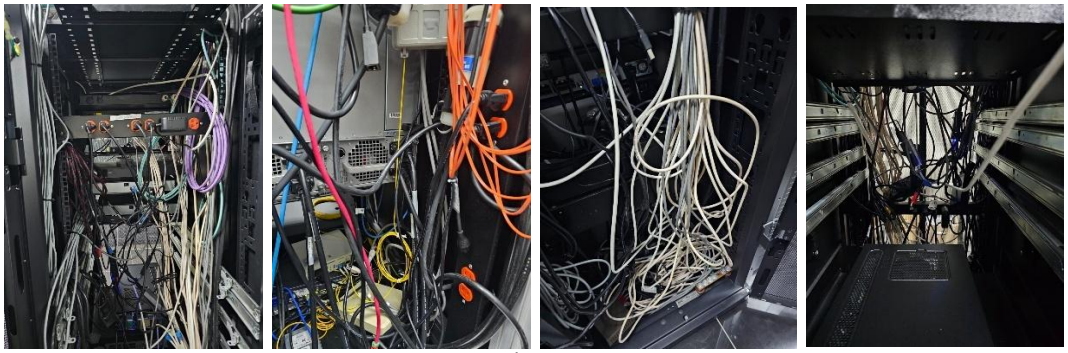
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas. **(Ver Hallazgo No. 3)**

2. Cableado estructurado

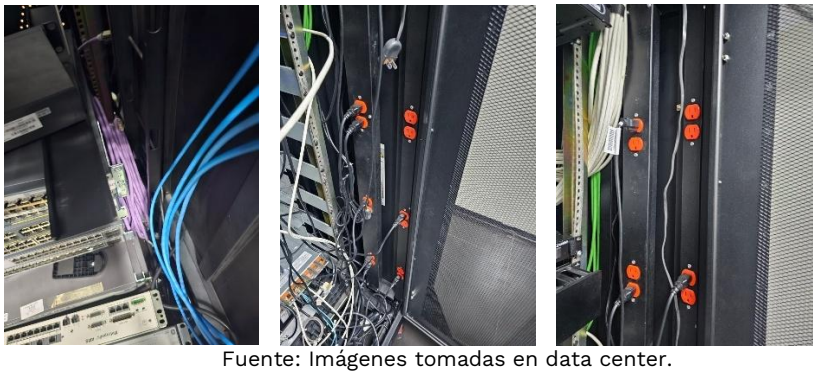
En verificación de las condiciones de cableado estructurado dentro de los racks donde se encuentran emplazados/instalados los distintos equipos de cómputo, comunicaciones, entre otros, se evidenciaron las siguientes condiciones:

a. Se evidenció la instalación de cableado fuera de los conductos laterales y/o verticales de los racks:



Fuente: Imágenes tomadas en data center.

b. Se evidenció el almacenamiento de cables de datos y eléctricos desconectados en racks del data center así como circuitos de conexión eléctrica sin etiquetado:



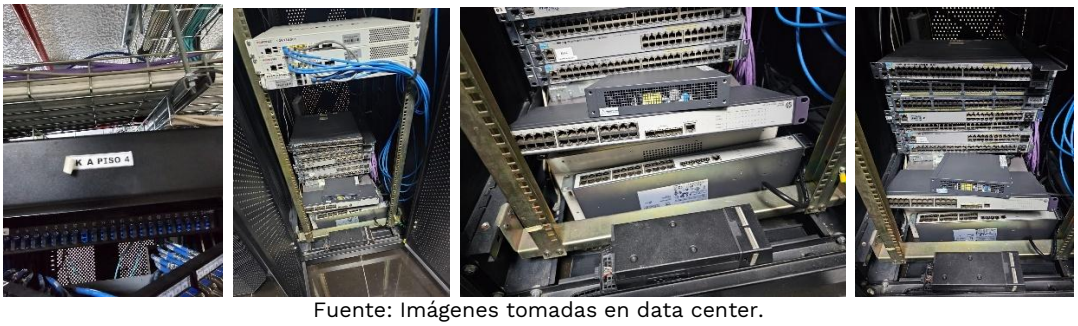
Fuente: Imágenes tomadas en data center.

Lo anterior evidencia debilidades en la aplicación del control A.11.2.3 Seguridad del cableado", del Modelo de Seguridad y Privacidad de la Información y del Anexo A. de la Norma ISO 27001, el cual establece:

"A.11.2.3 Seguridad del cableado, El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño."
(ver hallazgo No.3)

3. Equipos desconectados:

A partir de la verificación de la instalación de equipos en el Rack A PISO 4 se evidencio la presencia de distintos dispositivos no solamente desconectados, sino que adicionalmente no se encontraban emplazados/instalados dentro de las unidades del rack o colocados sobre bandejas de soporte según se muestra a continuación:



Fuente: Imágenes tomadas en data center.

Al respecto se solicitó confirmación de los registros de cambios asociados a la desinstalación de los equipos, sin embargo, en las evidencias remitidas por el Grupo de Trabajo de Tecnología, no se evidenció el registro de formatos de cambio, por otra parte según se confirmó por el área auditada tampoco se cuenta con un

procedimiento de “Gestión de cambio” en concordancia con el lineamiento “MGGTI.LI.GO.04 - Gestión de cambios” del modelo de referencia de Arquitectura Empresarial adicionalmente se pone de presente que existen debilidades en la implementación del control A.12.1.2 Gestión de cambios del Modelo de Seguridad y Privacidad de la Información y del Anexo A. de la Norma ISO 27001, el cual establece:

“**A.12.1.2 Gestión de cambios** Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento que afectan la seguridad de la información”.

De otra parte, se observó que algunos de los equipos no cuentan con placa de inventario de la entidad según se observa en las siguientes imágenes:

Fuente: Imágenes tomadas en data center.

Al respecto, según lo confirmado por la dependencia auditada los equipos sin placa pertenecen a los proveedores que en su momento prestaron servicios para la Entidad, los cuales no tienen una relación contractual vigente con el ministerio, sin embargo, son los proveedores quienes pueden retirarlos y hacer disposición final de los mismos.

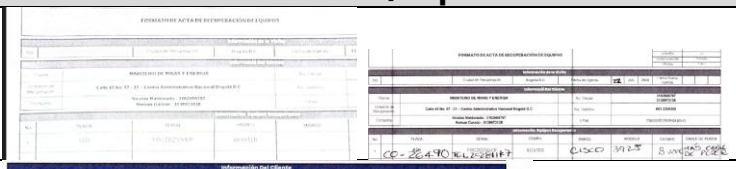
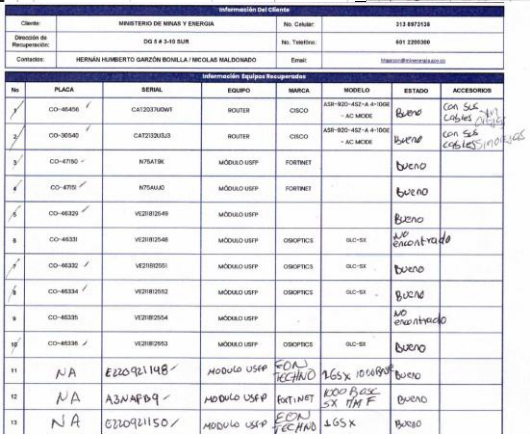
Ante esta situación la Oficina de Control Interno solicitó los soportes de retiro de equipos por parte de proveedores anteriores, ante lo cual se entregaron los siguientes documentos:

1. Acta de recuperación de Equipos Min. Minas y Energia ifx.pdf
2. actas retiro proveedores claro ufinet.pdf

3. MINISTERIO DE MINAS Y ENERGÍA_CAN_01032024 ifx.pdf
4. MINISTERIO DE MINAS Y ENERGÍA_SOACHA_05032024 if.pdf
5. MINISTERIO DE MINAS Y ENERGÍA_TEUSAQUILLO_01032024 ifx.pdf

Los soportes anteriormente referenciados evidencian que se han realizado actividades de devolución/recuperación de equipos por parte de proveedores, sin embargo, dichas acciones no dan alcance a la totalidad de equipos, toda vez que se encontraron en el desarrollo de la visita realizada en la vigencia 2025.

De otra parte, se observan los siguientes aspectos que pueden incidir en la gestión de registro y entrega o devolución de equipos a proveedores.

Aspecto Verificado	Evidencia /Soporte
1. Falta de legibilidad de los soportes	
2. Se evidenciaron casos en los que el proveedor manifestó en los reportes, que el equipo no fue encontrado en las instalaciones del cliente.	

Información Del Cliente

Cliente:	MINISTERIO DE MINAS Y ENERGIA	No. Celular:	313 8972138
Dirección de Recuperación:	DG 8 # 3-10 SUR	No. Telefono:	601 2200300
Contactos:	HERNÁN HUMBERTO GARZÓN BONILLA / NICOLAS MALDONADO	Email:	

Información Equipos Recuperados

No	PLACA	SERIAL	EQUIPO	MARCA	MODELO	ESTADO	ACCESORIOS
1	CO-46456	CAT2037U0WT	ROUTER	CISCO	ASR-920-4SZ-A 4-10GE - AC MODE	Bueno	con SUS CABLES
2	CO-36540	CAT2132U3J3	ROUTER	CISCO	ASR-920-4SZ-A 4-10GE - AC MODE	Bueno	con SUS CABLES
3	CO-47150	N75ATSK	MÓDULO USFP	FORTINET		bueno	
4	CO-4715	N75AUJD	MÓDULO USFP	FORTINET		bueno	
5	CO-46329	VE2181I2549	MÓDULO USFP			Bueno	
6	CO-46331	VE2181I2548	MÓDULO USFP	OSOPTICS	GLC-SX	NO encontrado	
7	CO-46332	VE2181I2551	MÓDULO USFP	OSOPTICS	GLC-SX	bueno	
8	CO-46334	VE2181I2552	MÓDULO USFP	OSOPTICS	GLC-SX	Bueno	
9	CO-46335	VE2181I2554	MÓDULO USFP			NO encontrado	
10	CO-46336	VE2181I2553	MÓDULO USFP	OSOPTICS	GLC-SX	bueno	
11	NA	E2209211148	MODULO USFP	FOR TECHNO	1GSX	Bueno	
12	NA	A3NAFD9	MODULO USFP	FORTINET	1000 BASE SX TAA F	bueno	
13	NA	E2209211150	MODULO USFP	FOR TECHNO	1GSX	Bueno	

Esta situación, sumada a la ausencia del procedimiento de Disposición de residuos tecnológicos confirmada por el área auditada, expone debilidades en la gestión de cambios asociados a la instalación/desinstalación de equipos y servicios del data center y afecta la adecuada disposición de residuos electrónicos lo que evidencia incumplimiento del lineamiento MGGTI.LI.ST.12 Disposición de residuos tecnológicos, del Modelo de Referencia de Arquitectura Empresarial, el cual establece: “La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, siguiendo las directrices de las áreas administrativas debe gestionar la correcta disposición de residuos tecnológicos de acuerdo con el Plan Institucional de Gestión Ambiental y teniendo en cuenta los lineamientos técnicos con los que cuente el gobierno nacional.” Ver **(Hallazgo No.3)**

HALLAZGO Nº 3 – Debilidades en la aplicación de Controles de Seguridad Física

Condición:

En el desarrollo de las visitas a los datacenter principal y alterno, se evidenciaron las siguientes situaciones que representan debilidades en la aplicación de controles de seguridad física:

1. Se evidenció agrietamiento/fractura en una de las paredes del centro de datos tanto a nivel horizontal (a nivel del techo) como vertical.
2. Sistemas de sujeción (chazos y tornillos) de las bandejas, ductos y escalerillas de cableado con condiciones de degaste (anclaje en techo agrietado, oxidación, tornillos sueltos)
3. Se identificó la presencia de elementos inflamables dentro de los racks.
4. Se evidenció la instalación de cableado fuera de los conductos laterales y/o verticales de los racks.
5. Se evidenció el almacenamiento de cables de datos y eléctricos desconectados en racks del data center así como circuitos de conexión eléctrica sin etiquetado
6. En el Rack A PISO 4 se evidencio la presencia de distintos dispositivos no solamente desconectados, sino que adicionalmente no se encontraban emplazados/instalados dentro de las unidades del rack o colocados sobre bandejas de soporte
7. Se solicitó confirmación de los registros de cambios asociados a la desinstalación de los equipos, sin embargo, en las evidencias remitidas por el Grupo de Trabajo de Tecnología, no se evidenció formatos o procedimientos de “cambio”.
8. Respecto al datacenter alterno, se identificó que se encuentra ubicado al lado de una polvorería situación que genera riesgos potenciales al complejo en el que se ubica el data Center; así mismo, se identificó que el sistema de aire acondicionado provisto en el data center alterno se encuentra alarmado, sin que se pudiera verificar sus condiciones de operación y mantenimiento, toda vez que no son de propiedad del ministerio; en este sentido según lo informado por el área auditada, se requirió implementar como contingencia un aire acondicionado portátil.
9. Se evidenció la instalación de cableado fuera de los conductos laterales y/o verticales de los racks:
10. Se evidenció el almacenamiento de cables de datos y eléctricos desconectados en racks del data center así como circuitos de conexión eléctrica sin etiquetado.
11. Se evidenció presencia de distintos dispositivos no solamente desconectados, sino que adicionalmente no se encontraban emplazados/instalados dentro de las unidades del rack o colocados sobre bandejas.
12. Según se confirmó por el área auditada no se cuenta con un procedimiento de “Gestión de cambio” ni de “Disposición de residuos tecnológicos”.

Criterio(s):

Resolución 500 de 2021 - Modelo de Seguridad y privacidad de la Información y Norma ISO 27001, Anexo A, controles:

“A.11.2.1 Ubicación y protección de los equipos”:
“Los equipos deben estar ubicados, y protegidos para reducir los riesgos de amenazas, peligros ambientales y las posibilidades de acceso no autorizado.”

“A.11.2.3 Seguridad del cableado”
“El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.”

“A.12.1.2 Gestión de cambios”
“Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento que afectan la seguridad de la información”.

“A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.”
“Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.”

“A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.”
“La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas”.

Resolución 1978 de 2023 anexo 1 -Modelo de referencia de Arquitectura Empresarial Lineamientos:

“MGGTI.LI.GO.04 - Gestión de cambios”
“La dirección de tecnologías y Sistemas de la información o quien haga sus veces debe definir e implementar formalmente un procedimiento de control de cambios”.

“MGGTI.LI.ST.12 Disposición de residuos tecnológicos”
“La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, siguiendo las directrices de las áreas administrativas debe gestionar la correcta disposición de residuos tecnológicos de acuerdo con el Plan Institucional de Gestión Ambiental y teniendo en cuenta los lineamientos técnicos con los que cuente el gobierno nacional.”

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Debilidades en el seguimiento a las actividades de instalación y/o mantenimiento realizadas al interior de los data center principal y alterno.
- Debilidades en la aplicación de controles de monitoreo y seguimiento a los registros, estados y documentación de actividades relacionadas con la entrega de equipos a proveedores, al final de los contratos.
- Posible falta de adopción de lineamientos, políticas, manuales, procedimientos entre otros para guiar las actividades de administración, seguimiento y control de los datacenter.
- Posible falta de conocimiento, habilidades y/o competencias del personal del Grupo

de Trabajo de Tecnología en marcos metodológicos y buenas prácticas de gestión de servicio y mesas de ayuda.
- Posible ausencia de mecanismos de verificación y controles detectivos de afectación estructural de los edificios en los que se encuentran ubicados los datacenter principal y alterno.
- Falta de trazabilidad de las actividades realizadas por los contratistas con respecto a las situaciones de alarma o falla de sistemas de la Entidad.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

La no atención oportuna de los casos puede implicar:

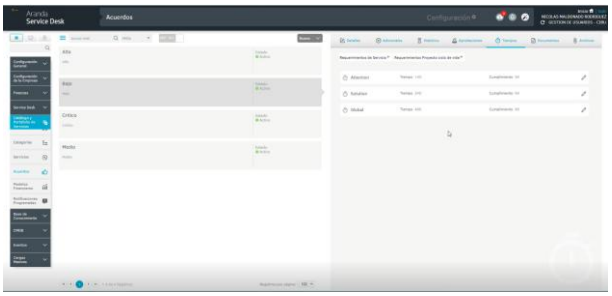
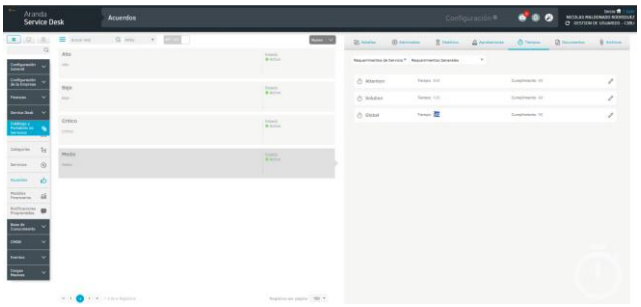
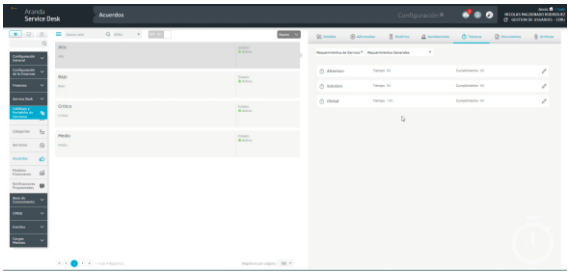
- Afectación de las actividades misionales, estratégicas y de apoyo de los distintos usuarios de la Entidad.
- Afectación económica y/o reputacional por la posible materialización de riesgos de seguridad de la información.
- Posible afectación a los activos de información de la Entidad.

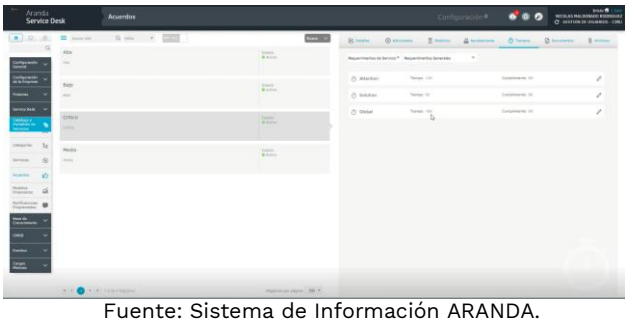
Recomendación(nes) específica(s):

- Fortalecer el diseño y aplicación de controles asociados a la gestión y operación de la mesa de ayuda.
- Fortalecer habilidades y competencias del personal del Grupo de Trabajo de Tecnología en marcos metodológicos y buenas prácticas de gestión de servicio y mesas de ayuda.
- Fortalecer el seguimiento y monitoreo del cumplimiento de los acuerdos de niveles de servicios – ANS, para los casos gestionados por la mes de ayuda.
- Evaluar la pertinencia de adoptar los lineamientos de la guía MGGTI.G.ST – Gestión de Servicios de TI (https://www.mintic.gov.co/arquitecturaempresarial/630/articles-237663_recurso_1.pdf), la cual forma parte de las guías de implementación del modelo de referencia de arquitectura empresarial de Mintic en su versión 3.0.
- Evaluar la pertinencia de reubicar el datacenter principal y/o alterno.
- Fortalecer el análisis de riesgo y controles detectivos ante posibles fallas estructurales y de seguridad física de los edificios en los que se encuentran los DataCenter Principal y alterno.

2. Operación de la mesa de Ayuda

Se evidenció en el desarrollo de la auditoría que los casos gestionados por la mesa de ayuda se registran en la herramienta Aranda, en este sentido dentro de la sesión adelantada con el proceso auditado el pasado lunes 12 de mayo de 2025, se verificaron los acuerdos de niveles de servicio configurados en la herramienta, encontrando lo siguiente:

Descripción ANS	Evidencia de configuración de ANS en ARANDA
Para los casos identificados con el Nivel de Atención BAJO: se definen los siguientes tiempos: Atención: 140 minutos Solución: 240 minutos Global: 480 minutos – (8 horas) Es de anotar, que según lo expuesto en la sesión de auditoría el tiempo global es equivalente a la sumatoria del tiempo de atención y el tiempo de solución; sin embargo, en este caso se observa que el tiempo Global es superior a 380 minutos (sumatoria de tiempo de atención y global), lo que evidencia una inconsistencia en la configuración del ANS dentro de la herramienta.	 Fuente: Sistema de Información ARANDA.
Para los casos identificados con el Nivel de Atención MEDIO: se definen los siguientes tiempos: Atención: 240 minutos Solución: 120 minutos Global: 360 minutos (6 horas) Es de anotar, que según lo expuesto en la sesión de auditoría el tiempo global es equivalente a la sumatoria del tiempo de atención y el tiempo de solución; en este caso se evidencia que el tiempo Global tiene una configuración de ANS coherente con la definición dada dentro de la herramienta.	 Fuente: Sistema de Información ARANDA.
Para los casos identificados con el Nivel de Atención ALTO: se definen los siguientes tiempos: Atención: 60 minutos Solución: 90 minutos Global: 120 minutos (2 horas)	 Fuente: Sistema de Información ARANDA.

Descripción ANS	Evidencia de configuración de ANS en ARANDA
Es de anotar, que según lo expuesto en la sesión de auditoría el tiempo global es equivalente a la sumatoria del tiempo de atención y el tiempo de solución; sin embargo, en este caso se observa que el tiempo Global es inferior a 150 minutos (sumatoria de tiempo de atención y global), lo que evidencia una inconsistencia en la configuración del ANS dentro de la herramienta.	
Para los casos identificados con el Nivel de Atención CRITICO: se definen los siguientes tiempos: Atención: 120 minutos Solución: 60 minutos Global: 180 minutos (1.5 horas) Es de anotar, que según lo expuesto en la sesión de auditoría el tiempo global es equivalente a la sumatoria del tiempo de atención y el tiempo de solución; en este caso se evidencia que el tiempo Global tiene una configuración de ANS coherente con la definición dada dentro de la herramienta.	 Fuente: Sistema de Información ARANDA.

En referencia a lo anteriormente analizado se evidencian inconsistencias en la configuración de los niveles de servicio identificados como “bajo” y “alto”, lo cual expone debilidades de control de los tiempos asociados al cumplimiento de los acuerdos de niveles de servicio, para la atención de casos por parte de la mesa de ayuda. **(ver Hallazgo No. 4)**

En adición a lo observado anteriormente, se verificaron los tiempos de solución de los casos a partir de los registros de las bases de datos de la herramienta Aranda, aportadas por el área auditada y correspondientes al periodo comprendido entre octubre y diciembre de la vigencia 2024, identificando los casos en los que se presentó una solución inferior a 3 días (posible cumplimiento de ANS) y superior a 3 días (posible incumplimiento de ANS), según se presenta en la tabla a continuación:

Vigencia 2024			
Mes	**Tiempo de Solución**	**Cantidad de Casos**	**% del total**
Octubre	inferior a 3 días	474	71,39%
	Superior a 3 días	190	28,61%
Total Octubre		**664**	**100%**
Noviembre	inferior a 3 días	327	81,55%
	Superior a 3 días	74	18,45%
Total Noviembre		**401**	**100%**
Diciembre	inferior a 3 días	77	60,63%
	Superior a 3 días	50	39,37%
Total Diciembre		**127**	**100%**

Fuente: Elaboración Propia

A partir de lo anterior se identificó el incumplimiento de ANS en el 28,61% de los casos solucionados en el mes de octubre, del 18,45% en el mes noviembre y del 39,37% en el mes de diciembre.

De manera análoga se realizó análisis de los casos solucionados en el periodo comprendido entre los meses de febrero y abril de la vigencia 2025, según se presenta en la tabla a continuación:

Vigencia 2025			
Mes	**Tiempo de Solución**	**Cantidad de Casos**	**% del total**
Febrero	inferior a 3 días	419	45,69%
	Superior a 3 días	498	54,31%
Total Febrero		**917**	**100%**
Marzo	inferior a 3 días	138	53,49%
	Superior a 3 días	120	46,51%
Total Marzo		**258**	**100%**
Abril	inferior a 3 días	69	28,05%
	Superior a 3 días	177	71,95%
Total Abril		**246**	**100%**

Fuente: Elaboración Propia

A partir de lo anterior se identificó el incumplimiento de ANS en el 54,31% de los casos solucionados en el mes de febrero, del 46,51% en el mes marzo y del 71,95% en el mes de abril. **(ver Hallazgo No. 4)**

Como complemento al análisis realizado se verificaron casos aleatorios registrados dentro de la herramienta ARANDA en los cuales se evidenció incumplimiento de ANS durante la sesión del 12 de mayo de 2025 en los cuales se observó lo siguiente:

No. Caso	Fecha de Apertura y Cierre	Observación
11199 (Ciclo de Vida – creación de usuario)	Apertura: 3/12/2024 10:42 Cierre: 9/12/2024 9:36 Tiempo transcurrido (6 días aproximadamente)	Se confirmó por parte del proceso auditado que no se cumplió el ANS y que la solución no depende únicamente del Grupo de TIC's, sin embargo, no se observa que se haya escalado o registrado observaciones dentro del caso.
11312 (Desactivación de usuario)	Apertura: 12/12/2024 12:16 Cierre: 17/12/2024 13:58 Tiempo transcurrido (5 días aproximadamente)	Se observa que en este caso se superan los tiempos de atención configurados como ANS dentro de la herramienta Aranda; sin embargo, se argumentó por parte de la dependencia auditada que se dá un tiempo de 5 días para la desactivación de los usuarios, tiempo que corresponde con la solución del caso.
11185 (Gestión de actualización de radicado - ARGO)	Apertura: 2/12/2024 16:09 Cierre: 6/12/2024 13:40 Tiempo transcurrido (4 días aproximadamente)	Se identificó que el caso corresponde a "ARGO" y por tanto no se encuentra dentro del alcance de gestión de la mesa de ayuda del Grupo TICS, sin embargo, fue cerrado por el contratista de mesa de ayuda y no fue escalado al Grupo correspondiente.
10721 (Creación de Servidor y asignación de políticas de backup)	Apertura: 12/11/2024 10:07 Cierre: 21/11/2024 09:13 Tiempo transcurrido (9 días aproximadamente)	Se confirmó por parte del proceso auditado que no se cumplió el ANS, sin embargo, no se observa que se haga diferenciación en los tiempos aplicables a distintas categorías o servicios que implícitamente pueden requerir mayor tiempo para su solución, como es el caso de la creación de nuevos servidores. De otra parte, se evidenció en la sesión la creación del servidor y la configuración y soporte se de ejecución de políticas y rutinas de backup del servidor creado
10667 (Creación de VPN)	Apertura: 6/11/2024 15:56 Cierre: 14/11/2024 08:31 Tiempo transcurrido (8 días aproximadamente)	Se observa que en este caso se superan los tiempos de atención configurados como ANS dentro de la herramienta Aranda; adicionalmente no se registra el detalle de la gestión y solución del caso dado que la persona que inició con la atención del caso ya no se encuentra laborando en la mesa de ayuda.
10256 (solicitud de copia de	Apertura: 18/10/2024 08:37 Cierre: 7/4/2025 08:31	Se observa que en este caso se superan los tiempos de atención configurados

No. Caso	Fecha de Apertura y Cierre	Observación
seguridad de un sitio)	Tiempo transcurrido (5 meses y 19 días aproximadamente)	como ANS dentro de la herramienta Aranda. Al respecto, la dependencia argumentó que el caso implicaba la copia de un sitio en sharepoint con un alto volumen de información lo que implicó distintas mesas de trabajo y tiempos de ejecución y verificación de la copia del sitio por parte de los usuarios. No obstante lo anterior, no se registra el detalle de la gestión y solución del caso dentro de la herramienta Aranda.

De otra parte, se identificaron situaciones relacionadas con la falta de registro de casos en la herramienta Aranda asociadas a:

1. Ausencia de registro asociado al evento de falla (intermitencia) del Sistema NEON el día 16 de abril de 2025, presentado en el desarrollo de la visita al Data Center alterno, para el cual se confirmó que no se creó el caso en la herramienta ARANDA durante el desarrollo de la sesión de auditoría del pasado 12 de mayo de 2025.
2. Se identificó alarma en UPS identificada en el desarrollo de la visita al data center principal (realizada el 11 de abril de 2025), para la cual se confirmó por escrito por parte del área auditada que “No se generó un caso Aranda dado que se generó una alarma auditiva la cual se revisó físicamente en el datacenter”
3. En lo relacionado con la alarma del equipo VNX 5400, se indicó por parte de la dependencia auditada que: “No se generó caso dado que la solución VNX 5400 no se encuentra con contrato de soporte. El motivo emana en que el producto ya alcanzo el EOL (End Of Life) y EOSL (End of Service), fin de vida y soporte de producto”.

A partir de todo lo expuesto se identificaron situaciones que evidencian:

1. Debilidades en la configuración de los tiempos asociados a los niveles de atención “bajo” y “alto”, dentro de la herramienta ARANDA.
2. Incumplimiento de acuerdos de niveles de servicio en la solución de casos de mesa de ayuda.
3. Debilidades en la asignación de casos y aplicación de guías y/o procesos y/o actividades de escalamiento.
4. Debilidades (ausencia en algunos casos) en el registro de casos y/o su documentación asociada en la herramienta Aranda.

Las anteriores situaciones evidencian el incumplimiento del lineamiento:

MGGTI.LI.ST.07 “Acuerdos de Nivel de Servicios” del Modelo de Gestión y Gobierno de TI el cual establece:

"La Dirección de Tecnología y Sistemas de la Información o quien haga sus veces, debe velar por el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos para los Servicios Tecnológicos." ***(ver Hallazgo No. 4)***

HALLAZGO Nº 4 - Incumplimiento de Acuerdos de Niveles de Servicio

Condición:

De acuerdo con el ítem "2. Operación de la mesa de ayuda" se evidenciaron las siguientes situaciones:

1. Inconsistencias en la configuración de los niveles de servicio identificados como "bajo" y "alto", lo cual expone debilidades de control de los tiempos asociados al cumplimiento de los acuerdos de niveles de servicio para la atención de casos por parte de la mesa de ayuda.
2. Resultados del análisis de tiempos de solución registrados en las bases de datos de atención de casos, reportadas por la Mesa de Servicios para las vigencias 2024 y 2025, según se detalla en las siguientes tablas:

Vigencia 2024			
Mes	**Tiempo de Solución**	**Cantidad de Casos**	**% del total**
Octubre	inferior a 3 días	474	71,39%
	Superior a 3 días	190	28,61%
Total Octubre		**664**	**100%**
Noviembre	inferior a 3 días	327	81,55%
	Superior a 3 días	74	18,45%
Total Noviembre		**401**	**100%**
Diciembre	inferior a 3 días	77	60,63%
	Superior a 3 días	50	39,37%
Total Diciembre		**127**	**100%**

Fuente: Elaboración Propia

Vigencia 2025			
Mes	**Tiempo de Solución**	**Cantidad de Casos**	**% del total**
Febrero	inferior a 3 días	419	45,69%
	Superior a 3 días	498	54,31%
Total Febrero		**917**	**100%**
Marzo	inferior a 3 días	138	53,49%
	Superior a 3 días	120	46,51%
Total Marzo		**258**	**100%**
Abril	inferior a 3 días	69	28,05%
	Superior a 3 días	177	71,95%

Vigencia 2025			
Mes	**Tiempo de Solución**	**Cantidad de Casos**	**% del total**
Total Abril		**246**	**100%**

Fuente: Elaboración Propia

3. Incumplimiento de ANS condiciones de registro y/o escalamiento en la herramienta Aranda para casos los casos 11199, 11312, 11185, 10721, 10667, 10256.
4. Ausencia de registros de casos en la herramienta Aranda en situaciones de alarma y falla y/o afectación de Sistemas de respaldo energético (UPS) y Sistema de Información Neón.

Criterio(s):

Resolución 1978 de 2023 – Artículo 3

"Artículo 3°. Principios del Marco de Referencia de Arquitectura Empresarial. La Versión 3 del Marco de Referencia de Arquitectura Empresarial, se desarrollará con fundamento en los principios consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998, 3° de la Ley 1437 de 2011, los principios de la Política de Gobierno Digital señalados en el artículo 2.2.9.1.1.3 del Decreto número 1078 de 2015 ***y adicionalmente los establecidos en el documento "MRAE.DM - DOCUMENTO MAESTRO", establecido en el Anexo 1 de la presente resolución.****" (negrita fuera de texto)*

Documento Maestro del MRAE – Modelo de Gestión y Gobierno de TI - Lineamiento MGGTI.LI.ST.07

"MGGTI.LI.ST.07 Acuerdos de Nivel de Servicios *La Dirección de Tecnología y Sistemas de la Información o quien haga sus veces, debe velar por el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos para los Servicios Tecnológicos."*

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- Debilidades en la configuración de ANS dentro de la herramienta de Gestión de casos/tickets (ARANDA).
- Debilidades en la aplicación de controles de monitoreo y seguimiento a los registros, estados y documentación de actividades relacionadas con la solución de casos atendidos por la mesa de ayuda.
- Posible falta de adopción de lineamientos, políticas, manuales, procedimientos entre otros para guiar las actividades y definir el alcance de los distintos niveles de atención, roles y responsabilidades inmersos en la operación de la mesa de ayuda.
- Posible falta de conocimiento, habilidades y/o competencias del personal del Grupo de Trabajo de Tecnología en marcos metodológicos y buenas prácticas de gestión de servicio y mesas de ayuda.

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

La no atención oportuna de los casos puede implicar:

- Afectación de las actividades misionales, estratégicas y de apoyo de los distintos usuarios de la Entidad.
- Afectación económica y/o reputacional por la posible materialización de riesgos de seguridad de la información.
- Falta de trazabilidad de las actividades realizadas por los contratistas con respecto a las situaciones de alarma o falla de sistemas de la Entidad.

Recomendación(nes) específica(s):

- Fortalecer el diseño y aplicación de controles asociados a la gestión y operación de la mesa de ayuda.
- Fortalecer habilidades y competencias del personal del Grupo de Trabajo de Tecnología en marcos metodológicos y buenas prácticas de gestión de servicio y mesas de ayuda.
- Fortalecer el seguimiento y monitoreo del cumplimiento de los acuerdos de niveles de servicios – ANS, para los casos gestionados por la mes de ayuda.
- Evaluar la pertinencia de adoptar los lineamientos de la guía MGGTI.G.ST – Gestión de Servicios de TI (https://www.mintic.gov.co/arquitecturaempresarial/630/articles-237663_recurso_1.pdf), la cual forma parte de las guías de implementación del modelo de referencia de arquitectura empresarial de Mintic en su versión 3.0.

Servicios de soporte de Mesa de Ayuda Prestados sin Contrato Formal

Ante las diversas desviaciones y debilidades de control detectadas en la Operación de la Mesa de Ayuda y a partir del desarrollo de las sesiones de auditoría se identificaron las siguientes situaciones:

1. En el desarrollo de la Auditoría se evidenció no solo la ejecución de actividades de soporte, registro y cierre de casos entre otras actividades, por parte del personal de mesa de ayuda; sino también la participación en las sesiones de auditoría y la argumentación de los pormenores de la operación para la vigencia 2025 (hasta la fecha de la sesión de auditoría 12 de mayo de 2025).
2. El proveedor “B2B” operó la mesa de ayuda en el marco de ejecución del contrato GGC- 643- 2024 hasta el 31 de diciembre de 2024.
3. En la actualidad (periodo comprendido desde el primero de enero, hasta el 12 de mayo de 2025 – fecha de la sesión de auditoría), no se evidenció la existencia de una relación contractual vigente entre el proveedor “B2B” (anterior proveedor del personal que operó la mesa de ayuda), ni directamente por parte de los contratistas con el Ministerio de Minas y Energía, según verificación realizada en el sistema de Información NEON.

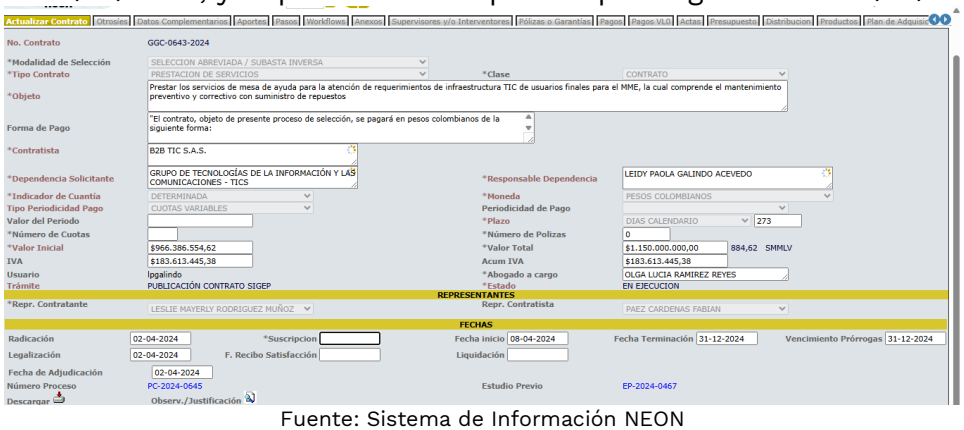
A partir de lo anterior se verificaron por parte de la Oficina de Control Interno los distintos antecedentes contractuales a fin de establecer si se realizó alguna prorroga y/o adición del

contrato que pudiese involucrar la extensión de la prestación de servicios a favor de la Entidad, evidenciando los siguientes aspectos relacionados con el contrato GGC- 643- 2024, suscrito con el proveedor B2B TIC, a partir de los registros del Sistema de Información NEON:

"Objeto Contractual: *Prestar los servicios de Mesa de Ayuda para la atención de requerimientos de la infraestructura TIC de usuarios finales para el MNE, lo cual comprende el mantenimiento preventivo y correctivo con suministro de repuestos"*

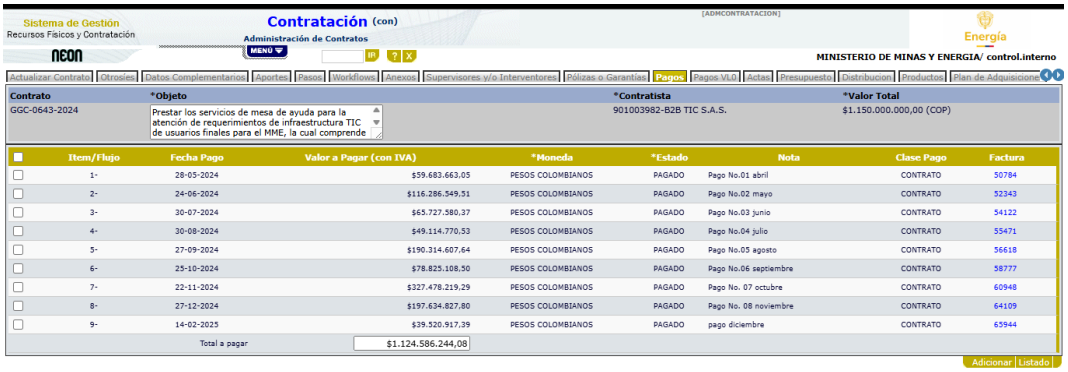
Verificada la información que reposa en el sistema de información NEON se observa:

1. Los Estudios Previos establecen Plazo de ejecución del contrato de nueve (9) meses o hasta el 31 de diciembre de 2024, lo primero que ocurra, contados a partir de la suscripción del acta de inicio.
2. Que, revisadas las obligaciones del contratista en los estudios previos, NO SE OBSERVÓ, la prestación de servicios de garantía o mantenimiento posteriores a la terminación del contrato.
3. Verificado el sistema de información NEON no obra solicitud de adición y prórroga del contrato previo a la terminación de este el 31/12/2024.
4. Se observa registrado en el sistema de información NEON la fecha de terminación del contrato 31/12/2024, y el plazo máximo para la prórroga de este 31/12/2024.



Fuente: Sistema de Información NEON

5. Se observan nueve (9) pagos en el sistema de información NEON asociados a los servicios prestados durante la ejecución del contrato, según se muestra en la imagen a continuación:



Fuente: Sistema de Información NEON

6. No se evidenciaron pagos dentro del expediente del Contrato GGC- 643- 2024 para la vigencia 2025.
7. No se evidenció la constitución de vigencias futuras para el Contrato GGC- 643- 2024 para la vigencia 2025.
8. Verificada la póliza del contrato, se observa que este obedece a la emisión inicial de la garantía, de acuerdo con las garantías exigidas en los estudios previos. Es importante recordar que la garantía debe extenderse o estar vigentes hasta la liquidación del contrato ARTÍCULO 2.2.1.2.3.1.12. Suficiencia de la garantía de cumplimiento Decreto 1082 de 2015. A la fecha de la verificación (13/05/2025) no se observó en NEON actualización de la póliza.

CLASE DE RIESGO	PORCENTAJE SOBRE EL VALOR DEL CONTRATO	VIGENCIA
Cumplimiento	20%	Por el plazo de ejecución del contrato y treinta (30) meses más, con vigencia a partir de la suscripción del contrato.
Calidad del servicio	20%	Por el plazo de ejecución del contrato y un (1) año más, contados a partir de la suscripción del contrato.
Calidad y correcto funcionamiento de los bienes	20%	Por el plazo de ejecución del contrato y un (1) año más, contados a partir de la suscripción del contrato.
Pago de Salarios, prestaciones sociales e indemnizaciones laborales	5%	Por el plazo de ejecución del contrato y tres (3) años más, contados a partir de la suscripción del contrato.

Fuente: Garantías del Contrato - Sistema de Información NEON

SEGUROS DEL ESTADO S.A.
NIT. 860.009.578-6

POLIZA DE SEGURO DE CUMPLIMIENTO ENTIDAD ESTATAL
DECRETO 1082 DE 2015

CIUDAD DE EXPEDICIÓN	SUCURSAL	COD.SUC	NO.PÓLIZA	ANEXO
BOGOTA, D.C.	ANTIGUO COUNTRY	21	21-44-101438800	0

FECHA EXPEDICIÓN DÍA	MES	AÑO	VIGENCIA DESDE DÍA	MES	AÑO	A LAS HORAS	VIGENCIA HASTA DÍA	MES	AÑO	A LAS HORAS	TIPO MOVIMIENTO
08	04	2024	05	04	2024	00:00	07	01	2026	23:59	EMISION ORIGINAL

DATOS DEL TOMADOR / GARANTIZADO

NOMBRE O RAZON SOCIAL	IDENTIFICACION
B2B TIC SAS	NIT: 901.003.982-1

DIRECCIÓN	CIUDAD	TELÉFONO
CR 67 # 167-51 OFICINA 610	BOGOTA, D.C., DISTRITO CAPITAL	6152689

DATOS DEL ASEGURADO / BENEFICIARIO

ASEGURADO / BENEFICIARIO	IDENTIFICACIÓN
LA NACION - MINISTERIO DE MINAS Y ENERGIA	NIT: 899.999.022-1

DIRECCION	CIUDAD	TELÉFONO
CL 43 NRO. 57 - 31	BOGOTA, D.C., DISTRITO CAPITAL	2200300

ADICIONAL:

OBJETO DEL SEGURO

CON SUJECIÓN A LAS CONDICIONES GENERALES DE LA PÓLIZA QUE SE ANEXAN MODIFICADO, QUE FORMAN PARTE INTEGRANTE DE LA MISMA Y QUE EL ASEGURADO Y EL TOMADOR DECLARAN HABER RECIBIDO Y HASTA EL LÍMITE DE VALOR ASEGURADO SEÑALADO EN CADA AMPARO, SUJETOS DEL ESTADO S.A., GARANTIZA:

CONTRATO GGC-643-2024 REFERENTE A PRESTAR LOS SERVICIOS DE MESA DE AYUDA PARA LA ATENCION DE REQUERIMIENTOS DE INFRAESTRUCTURA TIC DE USUARIOS FINALES PARA EL MME, LA CUAL COMPRENDE EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO CON SUMINISTRO DE REPUESTOS.

AMPAROS

RIESGO: SUMINISTRO DE BIENES

AMPAROS	VIGENCIA DESDE	VIGENCIA HASTA	SUMA ASEG/ACTUAL
CUMPLIMIENTO DEL CONTRATO	05/04/2024	07/07/2027	$230,000,000.00
PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES	05/04/2024	07/01/2028	$57,500,000.00
CALIDAD DEL SERVICIO	05/04/2024	07/01/2026	$230,000,000.00
CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES	05/04/2024	07/01/2026	$230,000,000.00

ACLARACIONES

Fuente: Sistema de Información NEON

Dado lo anterior se concluye que el contrato GGC- 643- 2024 estuvo vigente hasta el 31 de diciembre de 2024, sin que se presentaran adiciones y/o prorrogas para extender la operación de la mesa de ayuda por parte del personal contratado por la empresa “B2B TIC”, tampoco se identificó la constitución de vigencias futuras, ni se identificaron condiciones de garantía o mantenimiento de la operación posteriores a la terminación del contrato, así como tampoco se evidencia la extensión o modificación de la cobertura de las garantías inicialmente suscritas en favor de la Entidad.

Así las cosas, teniendo en cuenta que no se evidenciaron condiciones que sustentaran la continuidad de los servicios de mesa de ayuda prestados por parte del proveedor "B2B TIC" para la vigencia 2025, se indagó con el proceso auditado el detalle de la situación y posibles causas que motivaron la continuidad de la prestación de los servicios por parte del personal (contratistas), para los cuales no se identificó la existencia de un contrato laboral y/o de prestación de servicios vigente suscrito con la Entidad, ante lo cual, fue confirmado en la sesión de auditoría del 12 de mayo de 2025 por parte del área auditada lo siguiente:

1. *"Ellos están contratados todavía por B2B, pero pues, B2B con nosotros ya no tiene ningún vínculo contractual, lo que se hizo fue que ellos nos garantizaron pues el servicio de ellos sin costo adicional mientras salía el proceso".*
2. *"Como son prestación de servicios el contrato no se podía ni prorrogar ni extender y pues el nuevo contrato hasta ahora se está gestionando porque hemos tenido algunas dificultades en el proceso, pero ya pues lo estamos sacando adelante".*

También se indagó acerca de la facturación y pagos realizados al proveedor "B2B" ante lo que se confirmó, por parte de la dependencia auditada lo siguiente:

1. *Para 2025: "No hay facturación."*
2. *"El presupuesto que tenemos para 2024 es solo 2024, ó sea lo que es servicio no puede pasar vigencia"*
3. *Adicionalmente se confirmó que actualmente no se le está pagando al proveedor.*

Adicionalmente, con respecto a la vinculación de los contratistas que apoyan la gestión de la mesa de ayuda, se confirmó mediante correo electrónico que:

1. Actualmente se está realizando el trámite de vinculación mediante los siguientes procesos:
   "*EP-2025-1895 y EP 1896 con objeto Apoyar la gestión de infraestructura y servicios de TI mediante soporte técnico de primer nivel, garantizando la seguridad de la información y continuidad del negocio con protocolos de respuesta eficientes."*
2. Los contratistas: *"actualmente no tienen vínculo con la entidad, están en trámite de vinculación por prestación de servicios".*
3. *"La entidad ya no tiene contrato vigente con la empresa B2B y por tal motivo se esta gestionando el tramite de vinculación de las personas de mesa de ayuda por contrato de prestación de servicios, mientras se suscribe nuevo contrato para la gestión de mesa de ayuda (Proceso en trámite)".*

Por lo anterior expuesto, se configura la ocurrencia de hechos que han sido cumplidos por fuera de la formalidad del contrato, que pueden generar potencialmente un daño antijuridico, toda vez que, se evidenció la prestación de servicios por parte de personal (contratistas) en favor de la Entidad durante la vigencia 2025, sin tener una relación contractual vigente con el Ministerio, ya fuese de manera indirecta (subcontratados a través de otro proveedor) o de manera directa a través de contrato laboral y/o contrato de prestación de servicios suscrito con la Entidad, así como tampoco se cuenta con una relación contractual vigente entre el Ministerio y el proveedor "B2B TIC" empresa que contrató inicialmente al personal para el

desarrollo del objeto del contrato GGC- 643- 2024 el cuan finalizó su ejecución el 31/12/2024. **(ver Hallazgo No. 5)**

Así las cosas, se evidencia el incumplimiento de las directrices dadas por Manual de Contratación de la Entidad identificado con código T-GC-M-01, el cual en su numeral *"5.6 PROHIBICIONES PARA LOS SUPERVISORES E INTERVENTORES",* establece lo siguiente:

"5.6 PROHIBICIONES PARA LOS SUPERVISORES E INTERVENTORES
Los Supervisores e Interventores designados deben abstenerse de realizar las actividades que se describen a continuación:

(...)

e. *Autorizar la ejecución de objetos y prestaciones diferentes de las pactadas en el contrato.*
f. *Permitir el desarrollo del contrato sin el cumplimiento de los requisitos de ejecución.*
g. *Adoptar decisiones, celebrar acuerdo o suscribir documentos que tengan por finalidad o como efecto la modificación del contrato sin el lleno de los requisitos legales pertinentes(...)"*

Situación conlleva el desconocimiento de lo dispuesto por el artículo 41 de la Ley 80 de 1993, que dispone:

"DEL PERFECCIONAMIENTO DEL CONTRATO. Los contratos del Estado se perfeccionan cuando se logre acuerdo sobre el objeto y la contraprestación y éste se eleve a escrito.

Para la ejecución se requerirá de la aprobación de la garantía y de la existencia de las disponibilidades presupuestales correspondientes, salvo que se trate de la contratación con recursos de vigencias fiscales futuras de conformidad con lo previsto en la ley orgánica del presupuesto."

A su vez concordante con las disposiciones dadas por el artículo 71 del Decreto 111 de 1996, el cual, establece los siguiente:

"Todos los actos administrativos que afecten las apropiaciones presupuestales deberán contar con certificados de disponibilidad previos que garanticen la existencia de apropiación suficiente para atender estos gastos.

Igualmente, estos compromisos deberán contar con registro presupuestal para que los recursos con él financiados no sean desviados a ningún otro fin. En este registro se deberá indicar claramente el valor y el plazo de las prestaciones a las que haya lugar. Esta operación es un requisito de perfeccionamiento de estos actos administrativos.

En consecuencia, ninguna autoridad podrá contraer obligaciones sobre apropiaciones inexistentes, o en exceso del saldo disponible, o sin la autorización previa del Confis o por quien éste delegue, para comprometer vigencias futuras y la adquisición de compromisos con cargo a los recursos del crédito autorizados. (...)

Cualquier compromiso que se adquiera con violación de estos preceptos creará responsabilidad personal y pecuniaria a cargo de quien asuma estas obligaciones (Ley 38/89, artículo 86, Ley 179/94, artículo 49).” ***(Negrilla fuera de texto) (ver hallazgo No.5)***

Adicionalmente, esta situación evidencia debilidades en la aplicación del lineamiento MGGTI.LI.GO.09 Gestión de Proveedores de TI, el cual establece:

“La Dirección de tecnologías y Sistemas de la información o quien haga sus veces debe administrar todos los proveedores asociados con los proyectos y operación de TI. **Durante el proceso contractual se debe aplicar un esquema de dirección, supervisión, seguimiento, control y recibo a satisfacción de los bienes y servicios contratados, así como la transferencia de la información y conocimiento de los bienes y servicios de TI contratados alineados con las definiciones de la entidad** y los lineamientos del modelo de Gestión de Proyectos de TI (MGGTI).” **(negrita fuera de texto)**

HALLAZGO Nº 5 – Prestación de Servicios de soporte de Mesa de Ayuda Prestados sin Contrato Formal.
Condición:

Teniendo en cuenta que:

1. En el desarrollo de la Auditoría se evidenció no solo la ejecución de actividades de soporte, registro y cierre de casos entre otras actividades, por parte del personal de mesa de ayuda; sino también la participación en las sesiones de auditoría y la argumentación de los pormenores de la operación para la vigencia 2025 (hasta la fecha de la sesión de auditoría 12 de mayo de 2025).
2. El proveedor “B2B” operó la mesa de ayuda en el marco de ejecución del contrato GGC- 643- 2024 hasta el 31 de diciembre de 2024.
3. En la actualidad (periodo comprendido desde el primero de enero, hasta el 12 de mayo de 2025 – fecha de la sesión de auditoría), no se evidenció la existencia de una relación contractual vigente entre el proveedor “B2B” (anterior proveedor del personal que operó la mesa de ayuda), ni la existencia de relación contractual vigente de manera directa entre los contratistas que apoyan la gestión de la mesa de ayuda y el Ministerio de Minas y Energía, según verificación realizada en el sistema de Información NEON.

Y que adicionalmente no se evidenciaron condiciones que sustentaran la continuidad de los servicios de mesa de ayuda prestados por parte del proveedor “B2B TIC” para la vigencia 2025, se indagó con el proceso auditado el detalle de la situación y posibles causas que motivaron la continuidad de la prestación de los servicios por parte del personal (contratistas), para los cuales no se identificó la existencia de un contrato laboral y/o de prestación de servicios vigente suscrito con la Entidad, ante lo cual, fue confirmado en la sesión de auditoría del 12 de mayo de 2025 por parte del área auditada lo siguiente:

3. *“Ellos están contratados todavía por B2B, pero pues, B2B con nosotros ya no tiene ningún vínculo contractual, lo que se hizo fue que ellos nos garantizaron pues el servicio de ellos sin costo adicional mientras salía el proceso”.*

4. *"Como son prestación de servicios el contrato no se podía ni prorrogar ni extender y pues el nuevo contrato hasta ahora se está gestionando porque hemos tenido algunas dificultades en el proceso, pero ya pues lo estamos sacando adelante".*

También se indagó acerca de la facturación y pagos realizados al proveedor "B2B" ante lo que se confirmó, por parte de la dependencia auditada lo siguiente:

4. *Para 2025: "No hay facturación."*
5. *"El presupuesto que tenemos para 2024 es solo 2024, ó sea lo que es servicio no puede pasar vigencia"*
6. *Adicionalmente se confirmó que actualmente no se le está pagando al proveedor.*

Adicionalmente, con respecto a la vinculación de los contratistas que apoyan la gestión de la mesa de ayuda, se confirmó mediante correo electrónico que:

1. Actualmente se está realizando el trámite de vinculación mediante los siguientes procesos:
   "*EP-2025-1895 y EP 1896 con objeto Apoyar la gestión de infraestructura y servicios de TI mediante soporte técnico de primer nivel, garantizando la seguridad de la información y continuidad del negocio con protocolos de respuesta eficientes."*
2. Los contratistas: *"actualmente no tienen vínculo con la entidad, están en trámite de vinculación por prestación de servicios".*
3. *"La entidad ya no tiene contrato vigente con la empresa B2B y por tal motivo se está gestionando el trámite de vinculación de las personas de mesa de ayuda por contrato de prestación de servicios, mientras se suscribe nuevo contrato para la gestión de mesa de ayuda (Proceso en trámite)".*

Por lo anterior expuesto, se configura la ocurrencia de hechos que han sido cumplidos por fuera de la formalidad del contrato, que pueden generar potencialmente un daño antijuridico, toda vez que, se evidenció la prestación de servicios por parte de personal (contratistas) en favor de la Entidad durante la vigencia 2025, sin tener una relación contractual vigente con el Ministerio, ya fuese de manera indirecta (subcontratados a través de otro proveedor) o de manera directa a través de contrato laboral y/o contrato de prestación de servicios suscrito con la Entidad, así como tampoco se cuenta con una relación contractual vigente entre el Ministerio y el proveedor "B2B TIC" empresa que contrató inicialmente al personal para el desarrollo del objeto del contrato GGC- 643- 2024 el cuan finalizó su ejecución el 31/12/2024.

Criterio(s):

Ley 80 de 1993, "Por la cual se expide el Estatuto General de Contratación de la Administración PÚBLICA" artículo 41:

"DEL PERFECCIONAMIENTO DEL CONTRATO. Los contratos del Estado se perfeccionan cuando se logre acuerdo sobre el objeto y la contraprestación y éste se eleve a escrito.

Para la ejecución se requerirá de la aprobación de la garantía y de la existencia de las disponibilidades presupuestales correspondientes, salvo que se trate de la contratación con

recursos de vigencias fiscales futuras de conformidad con lo previsto en la ley orgánica del presupuesto."

Decreto 111 de 1996 "Por el cual se compilan la Ley 38 de 1989, la Ley 179 de 1994 y la Ley 225 de 1995 que conforman el estatuto orgánico del presupuesto".

artículo 71:

"**Todos los actos administrativos que afecten las apropiaciones presupuestales deberán contar con certificados de disponibilidad previos que garanticen la existencia de apropiación suficiente para atender estos gastos.**

Igualmente, estos compromisos deberán contar con registro presupuestal para que los recursos con él financiados no sean desviados a ningún otro fin. En este registro se deberá indicar claramente el valor y el plazo de las prestaciones a las que haya lugar. Esta operación es un requisito de perfeccionamiento de estos actos administrativos.

En consecuencia, ninguna autoridad podrá contraer obligaciones sobre apropiaciones inexistentes, o en exceso del saldo disponible, o sin la autorización previa del Confis o por quien éste delegue, para comprometer vigencias futuras y la adquisición de compromisos con cargo a los recursos del crédito autorizados.

(...)

Cualquier compromiso que se adquiera con violación de estos preceptos creará responsabilidad personal y pecuniaria a cargo de quien asuma estas obligaciones (Ley 38/89, artículo 86, Ley 179/94, artículo 49)." **(Negrilla fuera de texto)**

Manual de Contratación del Ministerio de Minas y Energía, código T-GC-M-01

"5.6 PROHIBICIONES PARA LOS SUPERVISORES E INTERVENTORES
Los Supervisores e Interventores designados deben abstenerse de realizar las actividades que se describen a continuación:

(...)

e. *Autorizar la ejecución de objetos y prestaciones diferentes de las pactadas en el contrato.*
f. *Permitir el desarrollo del contrato sin el cumplimiento de los requisitos de ejecución.*
g. *Adoptar decisiones, celebrar acuerdo o suscribir documentos que tengan por finalidad o como efecto la modificación del contrato sin el lleno de los requisitos legales pertinentes(...)"*

Modelo de Referencia de Arquitectura Empresarial.

Lineamiento MGGTI.LI.GO.09 Gestión de Proveedores de TI:

"La Dirección de tecnologías y Sistemas de la información o quien haga sus veces debe administrar todos los proveedores asociados con los proyectos y operación de TI. **Durante el proceso contractual se debe aplicar un esquema de dirección, supervisión, seguimiento, control y recibo a satisfacción de los bienes y servicios contratados, así como la transferencia de la información y conocimiento de los bienes y servicios de TI contratados alineados con las definiciones de la entidad** y los lineamientos del modelo de Gestión de Proyectos de TI (MGGTI)." **(negrita fuera de texto)**

Posible(s) causa(s) identificada(s) por la Oficina de Control Interno

- *Desconocimiento de los lineamientos dados por el Ministerio de Minas y Energía en relación con las responsabilidades, alcances de gestión y prohibiciones por parte de supervisores de contratos.*
- *Posible Falta de planeación y seguimiento a la ejecución oportuna de etapas precontractuales en procesos de contratación requeridos por la Entidad.*
- *Debilidades en la ejecución de controles de riesgo diseñados por el Grupo de Tecnología en materia de seguimiento a procesos contractuales.*

Posible(s) Consecuencias o efectos (s) identificado(s) por la Oficina de Control Interno

- *Posible daño antijuridico ante eventuales demandas por parte de proveedores y/o contratistas que prestaron en favor de la Entidad en la vigencia 2025 sin que se hayan realizado pagos por dichos conceptos.*
- *Posible materialización de riesgos de seguridad de la información al permitir acceso a sistemas de información, instalaciones, entre otros a personal sin un vínculo laboral vigente.*
- *Afectación de servicios en las condiciones requeridas por la Entidad en lo relacionado con la operación de la mesa de ayuda por ausencia y/o demoras en la formalización de contratos.*

Recomendación(nes) específica(s):

- Fortalecer las habilidades y competencias en materia de gestión contractual y presupuesta, para las personas del Grupo de Tecnología que fungen como supervisores de contratos al igual que aquellos que apoyan las labores de supervisión.
- Fortalecer los controles en materia de supervisión contractual y seguimiento a la planeación y ejecución del presupuesto a cargo del Grupo de Tecnología.

8.4 COMPONENTE INFORMACIÓN Y COMUNICACIÓN

Información del Proceso publicada en la página web

Se observa en primera instancia que el proceso es responsable de la gestión de los planes (i)Plan estratégico de Tecnologías de la Información – PETI, (ii) Plan de tratamiento de riesgos de seguridad de la información y (iii) Plan de seguridad y privacidad de la información, definidos como información mínima requerida por la ley 1712 de 2014 (ley de transparencia), en este sentido se verificó que dichos planes se encontraran publicados en la sección de transparencia de la Entidad en articulación con el Plan de acción como se pudo evidenciar en el link: https://www.minenergia.gov.co/es/ministerio/estrat%C3%A9gico/planes-y-programas/

También se evidenció que los mencionados planes fueron aprobados en sesión del comité Institucional de Gestión y Desempeño el día 28 de enero de 2025.

Para la vigencia 2024:

En la misma sección se dispone de un botón “Años Anteriores” el cual permite la consulta histórica de los planes anteriormente mencionados.

No obstante lo anterior, en la página web no se referencia la fecha de publicación de la Información, según puede apreciarse en las siguientes imágenes:

Fuente: Página Web de la Entidad

Lo anterior incumple el literal e) del numeral 2.4.1 Criterios generales de publicación de información pública del anexo 2 de la resolución 1519 de 2020, el cual indica:

“Todo documento o información debe indicar la fecha de su publicación en página web”. ***Ver Oportunidad de Mejora No. 1***

OPORTUNIDAD DE MEJORA Nº 1 – Fecha de Publicación de Documentación en la página web

Como resultado de la revisión de la información publicada en la página web, se identificó que el proceso de Gestión de Tecnologías de la Información y las Comunicaciones ha publicado los documentos: (i) Plan estratégico de Tecnologías de la Información – PETI, (ii)

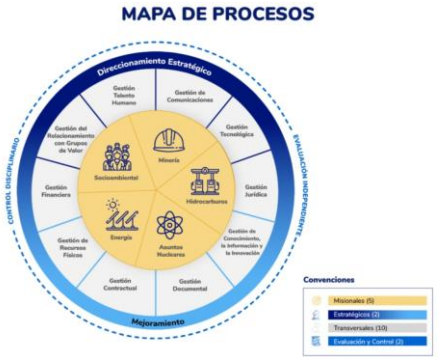
Plan de tratamiento de riesgos de seguridad de la información y (iii) Plan de seguridad y privacidad de la información, sin embargo; no se referencia la fecha de publicación de la Información, en concordancia con el literal e) del numeral 2.4.1 Criterios generales de publicación de información pública del anexo 2 de la resolución 1519 de 2020.

Recomendación(nes) específica(s):

- *Fortalecer el conocimiento del Grupo de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones en lo relacionado con los lineamientos de la Resolución 1519 de 2020 y sus anexos.*
- *Definir lineamientos y condiciones de publicación de contenidos de la Sección de transparencia, teniendo en cuenta los lineamientos descritos en el numeral 2.4.1 Criterios generales de publicación de información pública del anexo 2 de la resolución 1519 de 2020, relacionados con la información publicada en la sección de Transparencia de la Entidad.*

De otra parte, verificada la información del proceso publicada en la página web, se evidenció lo siguiente:

La información del sistema integrado de gestión de la entidad se publica en el siguiente link: https://www.minenergia.gov.co/es/ministerio/gesti%C3%B3n/procesos-y-procedimientos/, dentro de la cual se identifica el mapa de procesos del Ministerio de Minas y Energía, según se muestra en la imagen a continuación:

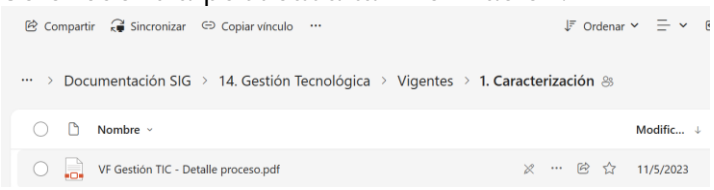


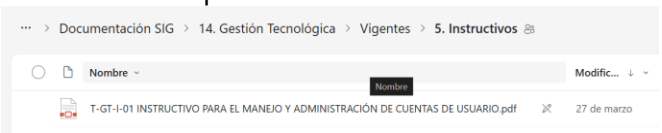
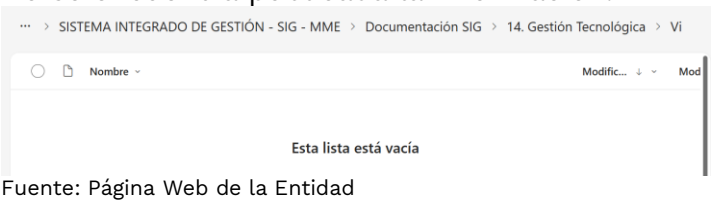
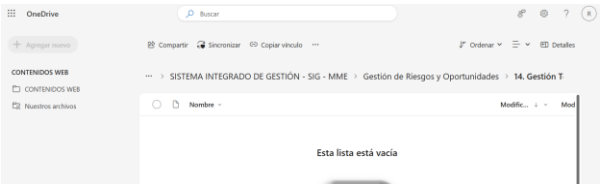
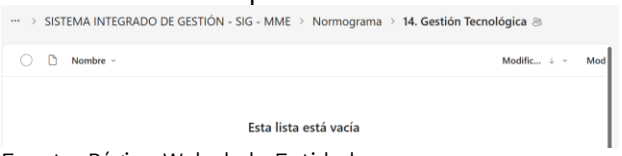
Fuente: Página Web de la Entidad

Al hacer clic en el proceso Gestión Tecnológica se identifica el tipo, objetivo, responsable y alcance del proceso y la documentación asociada, según se observa en la siguiente imagen.

Fuente: Página Web de la Entidad

Sin embargo, al hacer clic en los distintos botones se observa el siguiente comportamiento:

Aspecto/botón	Observación
caracterización	Se encuentra publicada la información:  Fuente: Página Web de la Entidad
Formatos	Se encuentra publicada la información:  Fuente: Página Web de la Entidad
Procedimientos	Se encuentra publicada la información:  Fuente: Página Web de la Entidad

Aspecto/botón	Observación
Manuales	No se encuentra publicada información:  Fuente: Página Web de la Entidad
Instructivos	Se encuentra publicada la información:  Fuente: Página Web de la Entidad
Guías	No se encuentra publicada la información:  Fuente: Página Web de la Entidad
Riesgos	No se encuentra publicada la información:  Fuente: Página Web de la Entidad
Normatividad	No se encuentra publicada la información:  Fuente: Página Web de la Entidad

A partir de lo anterior, se identifican secciones como Normatividad y Riesgos que no cuentan con los registros publicados, de otra parte, no se brinda claridad respecto a la existencia o no, de guías y manuales que puedan ser objeto de publicación como parte de la gestión del proceso. ***Ver Oportunidad de Mejora No. 2***

OPORTUNIDAD DE MEJORA Nº 2 - Publicación de Documentación del Proceso

Como resultado de la revisión de la información publicada en la página web asociada a la Gestión del proceso Auditado, se identifican secciones como Normatividad y Riesgos que no cuentan con los registros publicados, de otra parte, no se brinda claridad respecto a la existencia o no, de guías y manuales que puedan ser objeto de publicación como parte de la gestión del proceso.

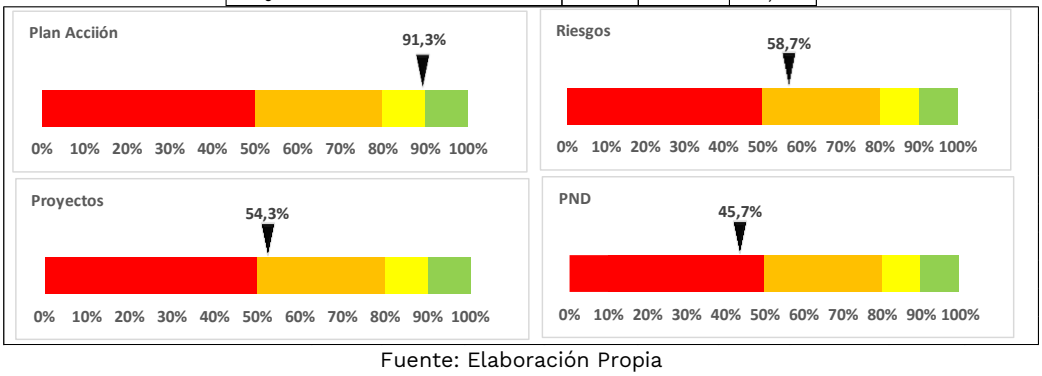
Recomendación(nes) específica(s):

- *Fortalecer la realización de actividades de control orientadas a la verificación de publicación de información del proceso en las secciones dispuestas para el Sistema de Integrado de Gestión – SI, de manera articulada con la OPGI, de manera que se asegure la consistencia entre los botones y enlaces dispuestos en la página web y los contenidos de las distintas secciones, micrositios, entre otros, que contienen información del proceso de Gestión de Tecnologías de la Información y las comunicaciones.*

8.5 COMPONENTE ACTIVIDADES DE MONITOREO

Se aplicó un instrumento de valoración el 19 de mayo 2025, dirigido al equipo de la unidad auditable (46 colaboradores), con el propósito de hacer un diagnóstico en cuanto a los mecanismos utilizados por para realizar seguimiento a la gestión, obteniendo los siguientes resultados:

Resultado general nivel de conocimiento			
Aspecto evaluado	**Total muestra**	**Cantidad Repuestas**	**%**
a. Seguimiento al plan de acción	46	42	**91,3%**
b. Monitoreo de riesgos	46	27	**58,7%**
c. Seguimiento a proyectos de inversión	46	25	**54,3%**
d. Seguimiento a metas del PND	46	21	**45,7%**



Fuente: Elaboración Propia

De lo anterior, se concluye que en mayor medida se realiza seguimiento a la gestión de la dependencia a través del plan de acción (91,3%), seguido por instrumentos o mecanismos

como, monitoreo a la gestión de riesgos con el 58.7%, seguimiento a proyectos de inversión con el 54,3% y por último a través del seguimiento a metas del Plan Nacional de Desarrollo con el 45.7%.

Frente a lo cual, es importante que, como resultado del seguimiento a través de dichos mecanismos se realice una autoevaluación que permita identificar los aspectos que requieren la adopción de estrategias orientadas a la mejora continua de la dependencia.

De otra parte, en el desarrollo de la presente auditoría, fue posible evidenciar que el proceso cuenta con diversos mecanismos de control y realiza seguimiento periódico de riesgos e indicadores; sin embargo, se identificaron desviaciones asociadas a:

1. Materialización de riesgos no reportadas en el monitoreo de riesgos.
2. Debilidades en el seguimiento y verificación del cumplimiento de acuerdos de niveles de servicio.
3. Debilidades en el registro, seguimiento y control de los cambios realizados sobre la plataforma tecnológica de la Entidad.
4. Debilidades en la aplicación de lineamientos en materia de gestión de procesos de contractuales.
5. Incumplimiento de términos para la implementación de lineamientos del Modelo de Referencia de Arquitectura Empresarial en el marco de la resolución 1978 de 2023.

Notas finales:

- ✓ La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Programa Anual de Auditoría, se encuentra limitada por restricciones de tiempo y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.
- ✓ La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por (dependencias proveedoras de información durante la auditoría interna), a través de solicitudes y consultas realizadas por la Oficina de Control Interno. Nuestro alcance no pretende corroborar la precisión de la información y su origen.
- ✓ Es necesario precisar que, las “Recomendaciones” propuestas en ningún caso son de obligatoria ejecución por parte de la Entidad, más se incentiva su consideración para los planes de mejoramiento a que haya lugar.
- ✓ La respuesta ante las situaciones observadas por la Oficina de Control Interno es discrecional de la Administración de la Entidad.

FIRMA
Julie Andrea Soto Laverde
JEFA OFICINA DE CONTROL INTERNO
Elaboró: Rigoberto Andrés Vaca Pardo - Contratista